



Informatica®  
10.5.3

# Installation for PowerCenter and Data Quality

© Copyright Informatica LLC 1998, 2023

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

Informatica, the Informatica logo, PowerCenter, and PowerExchange are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Subject to your opt-out rights, the software will automatically transmit to Informatica in the USA information about the computing and network environment in which the Software is deployed and the data usage and system statistics of the deployment. This transmission is deemed part of the Services under the Informatica privacy policy and Informatica will use and otherwise process this information in accordance with the Informatica privacy policy available at <https://www.informatica.com/in/privacy-policy.html>. You may disable usage collection in Administrator tool.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

The product includes ACE(TM) and TAO(TM) software copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (©) 1993-2006, all rights reserved.

This product includes Curl software which is Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://curl.haxx.se/docs/copyright.html>. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

This product includes ICU software which is copyright International Business Machines Corporation and others. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

This product includes OSSP UUID software which is Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissions and limitations regarding this software are subject to terms available at <http://www.opensource.org/licenses/mit-license.php>.

This software and documentation contain proprietary information of Informatica LLC and are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering of the software is prohibited. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC. This Software may be protected by U.S. and/or international Patents and other Patents Pending.

See patents at <https://www.informatica.com/legal/patents.html>.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

Publication Date: 2023-08-07

# Table of Contents

<b>Preface .....</b>	<b>13</b>
Informatica Resources. ....	13
Informatica Network. ....	13
Informatica Knowledge Base. ....	13
Informatica Documentation. ....	14
Informatica Product Availability Matrices. ....	14
Informatica Velocity. ....	14
Informatica Marketplace. ....	14
Informatica Global Customer Support. ....	14
 <b>Part I: Installation Getting Started.....</b>	 <b>15</b>
 <b>Chapter 1: Installation Getting Started.....</b>	 <b>16</b>
Checklist to Getting Started . ....	16
Installation Overview. ....	16
Installation Process. ....	17
Plan the Installation Option. ....	18
Plan the Installation Components. ....	19
Nodes. ....	19
Service Manager. ....	20
Application Services. ....	20
Databases. ....	20
User Authentication. ....	21
Secure Data Storage. ....	21
Domain Security. ....	22
Informatica Client Tools. ....	22
 <b>Part II: Before You Install the Services.....</b>	 <b>23</b>
 <b>Chapter 2: Before You Install the Services on UNIX or Linux. ....</b>	 <b>24</b>
Before You Begin Checklist . ....	24
Read the Release Notes. ....	25
Verify System Requirements. ....	25
Verify Temporary Disk Space and Permissions. ....	25
Review Patch Requirements on UNIX or Linux. ....	26
Verify Port Requirements . ....	27
Verify Distribution Package Requirements (Linux and UNIX). ....	29
Verify the File Descriptor Limit. ....	29
Verify Application Service Hardware Requirements. ....	30
Back Up the Data Transformation Files. ....	31

Configure POSIX Asynchronous I/O. . . . .	32
Review the Environment Variables. . . . .	32
Create a System User Account. . . . .	33
Set Up a Keystore File. . . . .	33
Download and Extract the Installer Files. . . . .	35
Verify Installer Code Signing. . . . .	35
Verify Installer Package Checksum on UNIX and Linux. . . . .	36
Verify the License Key. . . . .	36

## **Chapter 3: Before You Install the Services on Windows. . . . . 37**

Before You Install the Services on Windows Overview. . . . .	37
Read the Release Notes. . . . .	37
Verify System Requirements. . . . .	38
Verify Temporary Disk Space and Permissions. . . . .	38
Review the Patch Requirements. . . . .	38
Verify Port Requirements . . . . .	39
Verify Distribution Package Requirements (Windows). . . . .	40
Verify Application Service Hardware Requirements. . . . .	40
Back Up the Data Transformation Files. . . . .	42
Review the Environment Variables. . . . .	42
Create a System User Account. . . . .	43
Set Up Keystore and Truststore Files. . . . .	43
Download and Extract the Installer Files. . . . .	45
Verify Installer Code Signing. . . . .	45
Verify Installer Package Checksum on Windows. . . . .	46
Verify the License Key. . . . .	46

## **Chapter 4: Prepare for Application Services and Databases. . . . . 47**

Checklist to Prepare for Application Services . . . . .	47
Prepare for Application Services and Databases Overview. . . . .	48
Set Up Database User Accounts. . . . .	48
Identify Application Services by Product. . . . .	48
Domain Configuration Repository Database Requirements. . . . .	49
IBM DB2 Database Requirements. . . . .	50
Microsoft SQL Server Database Requirements. . . . .	51
Microsoft Azure SQL Database Requirements . . . . .	51
Oracle Database Requirements. . . . .	51
PostgreSQL Database Requirements . . . . .	52
Sybase Database Requirements. . . . .	52
Analyst Service . . . . .	53
Content Management Service. . . . .	54
Reference Data Warehouse Requirements. . . . .	54
Data Integration Service. . . . .	56

Data Object Cache Database Requirements. . . . .	57
Profiling Warehouse Requirements. . . . .	58
Workflow Database Requirements. . . . .	59
Metadata Manager Service. . . . .	62
Metadata Manager Repository Database Requirements. . . . .	62
IBM DB2 Database Requirements. . . . .	63
Microsoft SQL Server Database Requirements. . . . .	64
Oracle Database Requirements. . . . .	65
Split Domain for Metadata Manager. . . . .	65
Model Repository Service. . . . .	67
Model Repository Database Requirements. . . . .	67
IBM DB2 Database Requirements. . . . .	68
Microsoft Azure SQL Database Requirements. . . . .	69
Microsoft SQL Server Database Requirements. . . . .	69
Oracle Database Requirements. . . . .	70
PostgreSQL Database Requirements. . . . .	70
Monitoring Model Repository Service. . . . .	71
PowerCenter Integration Service. . . . .	71
PowerCenter Repository Service. . . . .	72
PowerCenter Repository Database Requirements. . . . .	72
IBM DB2 Database Requirements. . . . .	73
Microsoft SQL Server Database Requirements. . . . .	73
Oracle Database Requirements. . . . .	73
PostgreSQL Database Requirements . . . . .	74
Sybase ASE Database Requirements. . . . .	75
Search Service. . . . .	75
Configure Native Connectivity on Service Machines. . . . .	76
Install Database Client Software. . . . .	77
Configure Database Client Environment Variables. . . . .	78
 <b>Chapter 5: Prepare for Kerberos Authentication. . . . .</b>	 <b>81</b>
Checklist to Prepare for Kerberos Authentication . . . . .	81
Prepare for Kerberos Authentication Overview. . . . .	81
Set Up the Kerberos Configuration File. . . . .	82
Generate the Service Principal and Keytab File Name Format. . . . .	83
Service Principal Requirements at Node Level. . . . .	84
Service Principal Requirements at Process Level. . . . .	84
Running the SPN Format Generator . . . . .	85
Review the SPN and Keytab Format Text File. . . . .	86
Create the Service Principal Names and Keytab Files. . . . .	88
Troubleshooting the Service Principal Names and Keytab Files. . . . .	89

<b>Chapter 6: Record Information for Installer Prompts. ....</b>	<b>91</b>
Checklist to Record Installer Prompts. ....	91
Record Information for Installer Prompts Overview. ....	92
Domain. ....	92
Nodes. ....	93
Distribution Packages. ....	93
Application Services. ....	93
Databases. ....	94
Connection String to a Secure Database. ....	96
Secure Data Storage. ....	98
Kerberos. ....	98
 <b>Chapter 7: Introduction to the Services Installer. ....</b>	 <b>100</b>
Services Installer Tasks. ....	100
Secure Files and Directories. ....	100
Pre-install Utilities. ....	101
Run the Pre-Installation (i10Pi) System Check Tool in Console Mode. ....	101
Run the Pre-Installation (i10Pi) System Check Tool in Graphical Mode. ....	105
Run the Pre-Installation (i10Pi) System Check Tool in Silent Mode. ....	110
 <b>Part III: Run the Services Installer. ....</b>	 <b>111</b>
 <b>Chapter 8: Install Informatica Services in Console Mode. ....</b>	 <b>112</b>
Informatica Services Installation Overview. ....	112
Create a Domain. ....	112
Run the Installer. ....	112
Welcome to the Informatica Installer. ....	113
Welcome - Accept Terms and Conditions. ....	113
Component Selection. ....	113
License and Installation Directory. ....	114
Network Security - Service Principal Level. ....	114
Network Security - Kerberos Authentication. ....	115
Domain Selection. ....	116
Domain Security - Secure Communication. ....	119
Domain Configuration Repository. ....	120
Domain Security - Encryption Key. ....	125
Domain and Node Configuration. ....	126
Configure Informatica Application Services. ....	129
Configure the Model Repository Database. ....	129
Data Integration Service. ....	133
Configure the Monitoring Model Repository Database. ....	134
Content Management Service Parameters and Database. ....	138

Profiling Warehouse Database. . . . .	141
PowerCenter Repository Service and PowerCenter Integration Service. . . . .	143
Join a domain. . . . .	144
Run the Installer. . . . .	144
Welcome - Accept Terms and Conditions. . . . .	144
Component Selection. . . . .	145
Installation Prerequisites. . . . .	145
License and Installation Directory. . . . .	146
Service Principal Level. . . . .	146
Domain Selection. . . . .	147
Domain Security - Secure Communication. . . . .	147
Domain Configuration. . . . .	148
Domain Security - Encryption Key. . . . .	149
Join Domain Node Configuration. . . . .	149
Port Configuration. . . . .	150
Configure the Model Repository Database. . . . .	151
Data Integration Service. . . . .	155
PowerCenter Repository Service and PowerCenter Integration Service. . . . .	156
 <b>Chapter 9: Install Informatica Services in Graphical Mode. . . . .</b>	<b>157</b>
Install the Services in Graphical Mode Overview. . . . .	157
Create a Domain. . . . .	157
Run the Installer. . . . .	157
Welcome to the Informatica Installer. . . . .	158
Welcome - Accept Terms and Conditions. . . . .	159
License and Installation Directory. . . . .	160
Network Security - Service Principal Level . . . . .	163
Network Security - Kerberos Authentication. . . . .	164
Domain Selection. . . . .	166
Domain Security - Secure Communication. . . . .	172
Domain Configuration Repository . . . . .	174
Domain Security - Encryption Key. . . . .	177
Domain and Node Configuration. . . . .	178
Port Configuration. . . . .	181
Windows Service Configuration. . . . .	182
Configure Model Repository Service Database. . . . .	183
Configure Monitoring Model Repository Service Database. . . . .	188
Data Integration Service . . . . .	190
Content Management Service Parameters and Database. . . . .	192
Profiling Warehouse Connection Database. . . . .	196
PowerCenter Repository Service and the PowerCenter Integration Service . . . . .	199
Join a Domain. . . . .	200
Run the Installer. . . . .	200

Welcome to the Informatica Installer . . . . .	201
Welcome - Accept Terms and Conditions . . . . .	202
License and Installation Directory . . . . .	203
Network Security - Service Principal Level . . . . .	206
Network Security - Kerberos Authentication . . . . .	207
Domain Selection . . . . .	209
Domain Security - Secure Connection. . . . .	215
Domain Configuration . . . . .	217
Domain Security - Encryption Key . . . . .	218
Join Domain Node Configuration. . . . .	219
Port Configuration . . . . .	220
Windows Service Configuration. . . . .	221
Configure Model Repository Service Database . . . . .	222
Data Integration Service . . . . .	227
PowerCenter Repository Service and the PowerCenter Integration Service . . . . .	229
<b>Chapter 10: Run the Silent Installer. . . . .</b>	<b>231</b>
Installing in Silent Mode. . . . .	231
Configure the Properties File. . . . .	231
Run the Installer. . . . .	232
Encrypting Passwords in the Properties File. . . . .	232
<b>Chapter 11: Troubleshooting . . . . .</b>	<b>234</b>
Installation Troubleshooting Overview. . . . .	234
Resuming a Failed Installer Process. . . . .	234
Before You Resume the Installer. . . . .	235
Resume the Installer. . . . .	235
Troubleshooting with Installation Log Files. . . . .	235
Debug Log Files. . . . .	236
File Installation Log File. . . . .	236
Service Manager Log Files. . . . .	236
Troubleshooting Domains and Nodes. . . . .	237
Creating the Domain Configuration Repository. . . . .	237
Creating or Joining a Domain. . . . .	237
Starting Informatica. . . . .	238
Pinging the Domain. . . . .	238
Adding a License. . . . .	238
Troubleshooting Informatica Developer. . . . .	239
<b>Part IV: After You Install the Services. . . . .</b>	<b>240</b>
<b>Chapter 12: Complete the Domain Configuration. . . . .</b>	<b>241</b>
Checklist to Complete the Domain Configuration. . . . .	241



Complete the Domain Configuration Overview. . . . .	242
Verify Locale Settings and Code Page Compatibility. . . . .	242
Configure Locale Environment Variables. . . . .	242
Configure Environment Variables on UNIX or Linux. . . . .	243
Configure Informatica Environment Variables. . . . .	243
Configure Library Path Environment Variables. . . . .	244
Configure Kerberos Environment Variables. . . . .	245
<b>Chapter 13: Prepare to Create the Application Services. . . . .</b>	<b>246</b>
Checklist for Preparing to Create Application Services. . . . .	246
Create Directories for the Analyst Service. . . . .	247
Create a Keystore for a Secure Connection to a Web Application Service. . . . .	247
Log In to Informatica Administrator. . . . .	248
Troubleshooting the Login to Informatica Administrator. . . . .	248
Create Connections. . . . .	249
IBM DB2 Connection Properties. . . . .	250
Microsoft Azure SQL Database Connection Properties. . . . .	250
Microsoft SQL Server Connection Properties. . . . .	251
Oracle Connection Properties. . . . .	252
PostgreSQL Connection Properties. . . . .	253
Creating a Connection. . . . .	254
<b>Chapter 14: Create and Configure Application Services. . . . .</b>	<b>255</b>
Checklist to Create and Configure Application Services. . . . .	255
Create and Configure the Application Services Overview. . . . .	256
Create and Configure the Model Repository Service. . . . .	256
Create the Model Repository Service. . . . .	256
After You Create the Model Repository Service. . . . .	259
Create and Configure the Data Integration Service. . . . .	261
Create the Data Integration Service . . . . .	261
After You Create the Data Integration Service. . . . .	264
Create and Configure the PowerCenter Repository Service. . . . .	264
Create the PowerCenter Repository Service. . . . .	265
After You Create the PowerCenter Repository Service. . . . .	266
Create and Configure the PowerCenter Integration Service. . . . .	268
Create the PowerCenter Integration Service. . . . .	268
After You Create the PowerCenter Integration Service. . . . .	270
Create and Configure the Metadata Manager Service. . . . .	270
Create the Metadata Manager Service. . . . .	270
After You Create the Metadata Manager Service. . . . .	274
Create and Configure the Content Management Service. . . . .	274
Create the Content Management Service. . . . .	274
Create and Configure the Analyst Service. . . . .	276

Create the Analyst Service. . . . .	276
After You Create the Analyst Service. . . . .	278
Create and Configure the Search Service. . . . .	278
Create the Search Service. . . . .	278
<b>Part V: Informatica Client Installation. . . . .</b>	<b>281</b>
<b>Chapter 15: Install the Clients. . . . .</b>	<b>282</b>
Install the Clients Overview. . . . .	282
Before You Install. . . . .	283
Verify Installer Package Checksum . . . . .	283
Verify System Requirements. . . . .	283
Verify Third-party Requirements for Informatica Developer. . . . .	283
Verify Third-party Requirements for the PowerCenter Client. . . . .	284
Install the Clients. . . . .	284
After You Install. . . . .	285
Install Languages. . . . .	285
Configure the Client for a Secure Domain. . . . .	285
Configure the Developer Tool Workspace Directory. . . . .	286
Starting the PowerCenter Client. . . . .	287
Starting the Developer Tool. . . . .	287
<b>Chapter 16: Install in Silent Mode . . . . .</b>	<b>289</b>
Overview of Install in Silent Mode. . . . .	289
Configure the Properties File. . . . .	289
Run the Silent Installer. . . . .	290
<b>Part VI: Uninstallation. . . . .</b>	<b>291</b>
<b>Chapter 17: Uninstallation. . . . .</b>	<b>292</b>
Informatica Uninstallation Overview. . . . .	292
Rules and Guidelines for Uninstallation. . . . .	292
Uninstalling the Informatica Server in Console Mode. . . . .	293
Uninstalling Informatica Server in Silent Mode. . . . .	293
Uninstalling the Informatica Server in Graphical Mode. . . . .	294
Informatica Client Uninstallation. . . . .	294
Uninstalling Informatica Clients in Graphical Mode. . . . .	294
Uninstalling Informatica Clients in Silent Mode. . . . .	295
<b>Appendix A: Starting and Stopping Informatica Services. . . . .</b>	<b>297</b>
Starting and Stopping Informatica Services Overview . . . . .	297
Starting and Stopping the Informatica Services from the Console. . . . .	297
Stopping Informatica in Informatica Administrator. . . . .	298

Starting or Stopping Informatica from the Control Panel. . . . .	298
Starting or Stopping Informatica from the Start Menu. . . . .	298
Starting or Stopping Informatica from a Command Prompt. . . . .	299
Rules and Guidelines for Starting or Stopping Informatica. . . . .	299

## **Appendix B: Managing Distribution Packages..... 300**

Managing Distribution Packages Overview. . . . .	300
Before You Begin. . . . .	300
Install or Remove Distribution Packages in Console Mode. . . . .	301
Install or Remove Distribution Packages in Silent Mode. . . . .	302
After You Install. . . . .	302

## **Appendix C: Connecting to Databases from UNIX or Linux..... 304**

Connecting to Databases from UNIX or Linux Overview. . . . .	304
Connecting to an IBM DB2 Universal Database. . . . .	305
Configuring Native Connectivity. . . . .	305
Connecting to an Informix Database. . . . .	307
Configuring ODBC Connectivity. . . . .	307
Connecting to a Microsoft SQL Server Database. . . . .	308
Configuring SSL Authentication through ODBC. . . . .	308
Configuring Custom Properties for Microsoft SQL Server. . . . .	309
Connecting to a Netezza Database. . . . .	309
Configuring ODBC Connectivity. . . . .	309
Connecting to an Oracle Database. . . . .	311
Configuring Native Connectivity. . . . .	311
Connecting to a PostgreSQL Database. . . . .	313
Configuring Native Connectivity. . . . .	314
Configuring ODBC Connectivity. . . . .	315
Connecting to a Sybase ASE Database. . . . .	317
Configuring Native Connectivity. . . . .	317
Connecting to a Teradata Database. . . . .	319
Configuring ODBC Connectivity. . . . .	320
Connecting to a JDBC Data Source. . . . .	322
Connecting to an ODBC Data Source. . . . .	322
Sample odbc.ini File. . . . .	324

## **Appendix D: Connecting to Databases from Windows..... 331**

Connecting to Databases from Windows Overview. . . . .	331
Connecting to an IBM DB2 Universal Database from Windows. . . . .	332
Configuring Native Connectivity. . . . .	332
Connecting to an Informix Database from Windows. . . . .	332
Configuring ODBC Connectivity. . . . .	333
Connecting to Microsoft Access and Microsoft Excel from Windows. . . . .	333

Configuring ODBC Connectivity. . . . .	333
Connecting to a Microsoft SQL Server Database from Windows. . . . .	333
Configuring Native Connectivity. . . . .	333
Configuring Custom Properties for Microsoft SQL Server. . . . .	335
Connecting to a Netezza Database from Windows. . . . .	335
Configuring ODBC Connectivity. . . . .	335
Connecting to an Oracle Database from Windows. . . . .	336
Configuring Native Connectivity. . . . .	336
Connecting to a PostgreSQL Database. . . . .	337
Configuring Native Connectivity. . . . .	338
Configuring ODBC Connectivity . . . . .	338
Connecting to a Sybase ASE Database from Windows. . . . .	339
Configuring Native Connectivity. . . . .	339
Connecting to a Teradata Database from Windows. . . . .	340
Configuring ODBC Connectivity. . . . .	341
<b>Appendix E: Updating the DynamicSections Parameter of a DB2 Database. .</b>	<b>342</b>
DynamicSections Parameter Overview. . . . .	342
Setting the DynamicSections Parameter. . . . .	342
Downloading and Installing the DDconnect JDBC Utility . . . . .	342
Running the Test for JDBC Tool . . . . .	343
<b>Index. . . . .</b>	<b>344</b>

# Preface

Follow the instructions in *Installation for PowerCenter and Data Quality* to install Informatica services and the PowerCenter and Informatica Data Quality products. You can install Informatica services and clients on one or more machines. The guide includes pre- and post-requisite tasks and steps to install the Informatica services and clients for the Informatica domain. Prerequisite tasks include planning the environment, setting up databases, and verifying system requirements. Post-requisite tasks include additional application services and configuring environment variables.

## Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

### Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit <https://network.informatica.com>.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

### Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit <https://search.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

## Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit <https://docs.informatica.com>.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

## Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at <http://velocity.informatica.com>. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at [ips@informatica.com](mailto:ips@informatica.com).

## Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at <https://marketplace.informatica.com>.

## Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:

<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>.

To find online support resources on the Informatica Network, visit <https://network.informatica.com> and select the eSupport option.

# Part I: Installation Getting Started

This part contains the following chapter:

- [Installation Getting Started, 16](#)

# CHAPTER 1

## Installation Getting Started

This chapter includes the following topics:

- [Checklist to Getting Started , 16](#)
- [Installation Overview, 16](#)
- [Installation Process, 17](#)
- [Plan the Installation Option, 18](#)
- [Plan the Installation Components, 19](#)

### Checklist to Getting Started

This chapter contains high-level concepts and planning information related to installation. Use this checklist to track the completion of preliminary tasks.

☐ Understand high-level concepts:

- The installer description and process.
- Informatica domain terminology and components.

☐ Start high-level planning:

- Installation options. Review the installation options to know the product and options for installation.
- Installation components. Review the description of the installation components and the planning notes.

### Installation Overview

Welcome to the Informatica installer Informatica domain services and clients. The Informatica domain services consist of core services to support the domain and application services. The Informatica clients consist of thick and web client applications.

When you install the Informatica domain services, you are prompted to create a domain or to join a domain. The domain is a collection of nodes that represent the machines on which the application services run. The first time you run the installer, you must create the domain. If you install on a single machine, you create the Informatica domain and a gateway node on the machine. If you install on multiple machines, you create an Informatica domain and a gateway node during the first installation. During the installation on the additional machines, you create gateway or worker nodes that you join to the domain.



When you run the installer, it installs files for services. You can optionally create application services during the installation process, or you can manually create application services when the installation completes.

If you have other Informatica products installed, verify that the installed version is compatible with the version of the product that you are installing.

## Installation Process

The installation of the Informatica domain services and Informatica clients consists of multiple phases.

The installation process varies based on the products that you install. Consider the following high-level tasks of the installation process:

### **Perform pre-installation tasks.**

1. Plan the Informatica installation. Determine the products that you want to run in your environment. If you are creating a domain, consider the number of nodes in the domain, the application services that will run on each node, the system requirements, and the type of user authentication that the domain will use.
2. Prepare the databases required for repositories, warehouses, and catalogs. Verify the database requirements and set up the databases.
3. Set up the machines to meet system requirements to ensure that you can successfully install and run the Informatica services.
4. Determine security requirements for the domain, services, and databases.

### **Run the installer.**

When you run the installer, you can choose from different options based on your requirements.

### **Complete the configuration.**

1. Verify code page compatibility.
2. Configure environment variables.
3. Complete tasks required by the type of user authentication used by the domain.
4. Optionally, configure secure communication for the domain.
5. Create and configure application services.
6. Configure connections required by the application services.
7. Create the users and connections required by the application services.

### **Install the Informatica client tools.**

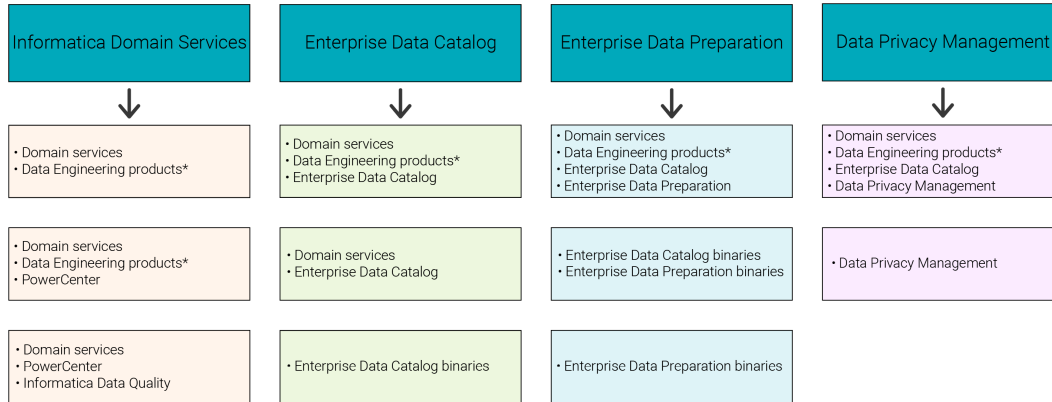
1. Verify the installation and third-party software requirements for the clients.
2. Use the client installer to install on Windows machines.
3. Configure required environment variables, and optionally install additional languages.

# Plan the Installation Option

Before you begin the planning and preparation for install, determine the type of installation that you want to run.

When you run the installer, you can choose from options in the Welcome panel based on the product or products that you want to install. The Components panel appears based on your product selection so you can choose product components.

The following image shows the products that you can install based on the installation options:



\*Data Engineering products include Data Engineering Integration, Data Engineering Quality, and Data Engineering Streaming.

Consider the different options available when you run the installer:

## Informatica domain services

To install the Informatica domain services, you can select the installation option 1 in the Components panel to install and configure Informatica domain services.

With the Informatica domain services installation, install from one of the following product options:

- Only the Data Engineering products for Integration, Quality, and Streaming
- Traditional products and the aforementioned Data Engineering products
- Only traditional products such as PowerCenter and Informatica Data Quality

When you install Informatica domain services, you can choose to create a domain or join a domain. Test Data Management is installed with both traditional and Data Engineering products.

## Enterprise Data Catalog

To install Enterprise Data Catalog, you can select the installation option 2 in the Components panel to install and configure Enterprise Data Catalog.

When you install Enterprise Data Catalog, choose from one of the follow options:

- Domain services, Data Engineering products, and Enterprise Data Catalog.
- Domain services and Enterprise Data Catalog.
- Only Enterprise Data Catalog binaries in an existing domain. After you install the binaries, you can run the installer again to configure the services.

## Enterprise Data Preparation

To install Enterprise Data Preparation, you can select the following installation option 3 in the Components panel to install and configure Enterprise Data Preparation.

When you install Enterprise Data Preparation, choose from one of the follow options:

- Data Engineering products, Enterprise Data Catalog, and Enterprise Data Preparation.
- Enterprise Data Catalog and Enterprise Data Preparation binaries in an existing domain. After you install the binaries, you can run the installer again to configure the services.
- Only Enterprise Data Preparation binaries in an existing domain with Enterprise Data Catalog. After you install the binaries, you can run the installer again to configure the services.

#### Data Privacy Management

To install Data Privacy Management, you can select the following installation option 4 in the Components panel to install and configure Data Privacy Management.

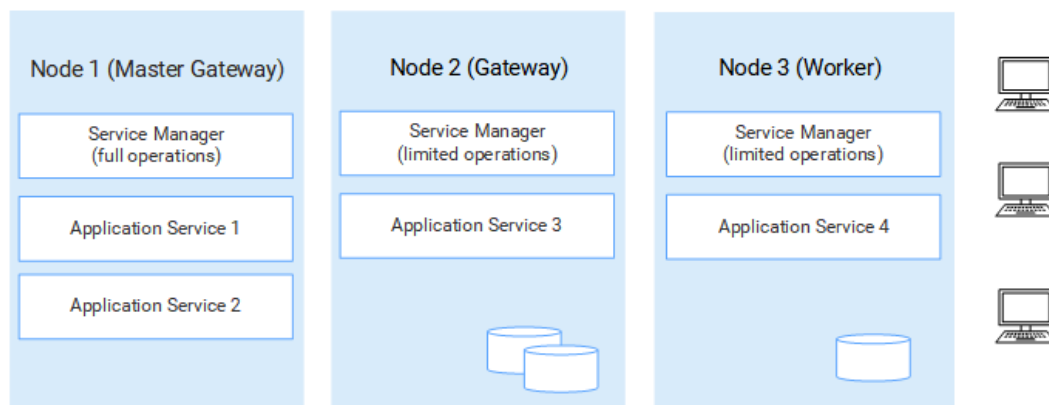
When you install Data Privacy Management, choose from one of the follow options:

- Data Engineering products, Enterprise Data Catalog, and Data Privacy Management.
- Data Privacy Management in an existing domain with Enterprise Data Catalog.

## Plan the Installation Components

An Informatica domain is a collection of nodes and services. A node is the logical representation of a machine in a domain. Services include the Service Manager that manages all domain operations and a set of application services that represent server-based functionality. The domain and some services require databases to write metadata and run-time results.

The following image shows a high-level architecture of a domain on multiple nodes:



## Nodes

The first time that you install the domain services, you create the Informatica domain and a gateway node. When you install the domain services on other machines, you create additional nodes that you join to the domain.

The domain has the following types of nodes:

- Gateway node. A gateway node is any node that you configure to serve as a gateway for the domain. A gateway node can run application services and it can serve as a master gateway node. The master gateway node is the entry point to the domain. You can configure more than one node as a gateway node, but only gateway node acts as the master gateway node at any given time.

- **Worker node.** A worker node is any node that you do not configure to serve as a gateway for the domain. A worker node can run application services, but it cannot serve as a gateway.

**When you plan the installation:** You need to plan the number and type of nodes that you need based on your service and processing requirements. If you have high availability, you will want to create more than one gateway node for fail-over functionality.

## Service Manager

The Service Manager is a service that manages all domain operations. The Service Manager runs on each node in the domain and performs domain functions, such as authentication, logging and application service management. The Service Manager on a gateway node performs more tasks than the Service Manager on a worker node.

**When you plan the installation:** Note that the Service Manager functionality is associated with the type of node.

## Application Services

Application services represent server-based functionality. An application service might be required or optional, and it might require access to a database.

When you run the installer, you can choose to create some services. After you complete the installation, you create other application services based on the license key generated for your organization.

**When you plan the installation:** When you plan the application services, you must account for the associated services that connect to the application service. You also must plan the relational databases that are required to create the application service.

## Databases

Some application services require databases to store metadata and to write run-time results. You need to create databases for the application services in the domain.

You can create the following databases:

### **Domain configuration repository database**

The domain configuration repository stores configuration and user information from a domain.

### **Reference data warehouse database**

The reference data warehouse stores the data values for reference table objects that you define in a Model repository. Configure a Content Management Service to identify the reference data warehouse and the Model repository.

### **Data object cache database**

The data object cache stores cached logical data objects and virtual tables for the Data Integration Service. Data object caching enables the Data Integration Service to access pre-built logical data objects and virtual tables.

### **Profiling warehouse database**

The profiling warehouse stores profiling and scorecard results. You need a profiling warehouse to perform profiling and data discovery.

### **Workflow database**

The workflow database stores run-time metadata for workflows using the Data Integration Service.

### Metadata Manager repository database

The Metadata Manager repository is a centralized location in a relational database that stores metadata from disparate metadata sources. It also stores the Metadata Manager warehouse and the models for each metadata source type.

### Model repository database

The Model repository stores data and metadata from the Informatica services and clients. Informatica client tools, such as Analyst tool and the Developer tool stores the data into the Model repository.

### Monitoring Model repository database

The Monitoring Model repository stores statistics for ad hoc jobs, applications, logical data objects, SQL data services, web services, and workflows created by Informatica clients and application services.

### PowerCenter repository database

The PowerCenter repository stores data and metadata from the PowerCenter services and clients. The PowerCenter Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

**When you plan the installation:** You need to create databases and database users required by application services.

## User Authentication

When you run the installer, you can choose the authentication to use for the domain.

The Informatica domain can use the following types of authentication to authenticate users in the domain:

- **Native.** Native user accounts are stored in the domain and can only be used within the domain. Native authentication is default.
- **LDAP.** LDAP user accounts are stored in an LDAP directory service and are shared by applications within the enterprise. You can configure LDAP authentication after you run the installer.
- **SAML.** You can configure Security Assertion Markup Language (SAML) authentication for the Administrator tool, the Analyst tool, and the Monitoring tool. You can configure SAML authentication after you run the installer.
- **Kerberos.** Kerberos user accounts are stored in an LDAP directory service and are shared by applications within the enterprise. If you enable Kerberos authentication during installation, you must configure the Informatica domain to work with the Kerberos Key Distribution Center (KDC).

**When you plan the installation:** You need to plan the type of authentication that you want to use in the domain. If you want the installer to configure Kerberos authentication, you must prepare the network prior to installation. You can also configure Kerberos after installation. Note that you cannot configure both SAML and Kerberos authentication.

## Secure Data Storage

Informatica encrypts sensitive data before it stores the data in the Informatica repositories.

When you create a domain, you must specify the encryption key directory. The installer generates an encryption key file named `siteKey` and stores it in a default directory or the directory you specify. All nodes in a domain must use the same encryption key.

**Important:** The installer also generates a unique site key. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.

## Domain Security

When you create a domain, you can enable options to configure security in the domain.

You can configure secure communication for the following domain components:

- Administrator tool. Configure a secure HTTPS connection for the Administrator tool. During installation, you can provide the keystore file to use for the HTTPS connection.
- Service Manager. Configure a secure connection between the Service Manager and other domain services. During installation, you can provide keystore and truststore files containing SSL certificates that you want to use.
- Domain configuration repository. You can secure the domain configuration repository with SSL protocol. During installation, you can provide the truststore file containing the SSL certificate that you want to use.

**When you plan the installation:** Determine the level of security that you want to configure for the domain components. If you decide to configure security for the domain, you must know the location and password for the keystore and truststore files. If you decide to use Kerberos authentication for the Informatica domain, you must work with the Kerberos administrator to set up the user and service principals required by the domain.

## Informatica Client Tools

You use Informatica clients to access underlying Informatica functionality in the domain. The clients make requests to the Service Manager and to application services.

The Informatica clients consist of thick client applications and thin or web client applications that you use to access services and repositories in the domain.

The following table describes the tools for PowerCenter:

Informatica Client	Description
Informatica Developer (the Developer tool)	A thick client application to create and run data objects, mappings, profiles, and workflows.
Informatica Administrator (the Administrator tool)	A web application to manage the domain and application services.
Informatica Analyst (the Analyst tool)	A web application to analyze, cleanse, integrate, and standardize data in an enterprise.
PowerCenter Client	A thick client application to create and run mappings, sessions, and workflows.

**When you plan the installation:** Determine how many instances of the PowerCenter Client and the Developer tool that you want to install. You do not need to plan for the web client applications.

# Part II: Before You Install the Services

This part contains the following chapters:

- [Before You Install the Services on UNIX or Linux, 24](#)
- [Before You Install the Services on Windows, 37](#)
- [Prepare for Application Services and Databases, 47](#)
- [Prepare for Kerberos Authentication, 81](#)
- [Record Information for Installer Prompts, 91](#)
- [Introduction to the Services Installer, 100](#)

## CHAPTER 2

# Before You Install the Services on UNIX or Linux

This chapter includes the following topics:

- [Before You Begin Checklist , 24](#)
- [Read the Release Notes, 25](#)
- [Verify System Requirements, 25](#)
- [Back Up the Data Transformation Files, 31](#)
- [Configure POSIX Asynchronous I/O, 32](#)
- [Review the Environment Variables, 32](#)
- [Create a System User Account, 33](#)
- [Set Up a Keystore File, 33](#)
- [Download and Extract the Installer Files, 35](#)
- [Verify the License Key, 36](#)

## Before You Begin Checklist

This chapter contains preliminary tasks that you must complete. Use this checklist to track preliminary tasks before you prepare for services.

- ☐ Read the Informatica Release Notes for updates to the installation and upgrade process.
- ☐ Verify system requirements:
  - Verify sizing requirements based upon your processing and concurrency requirements.
  - Review the patch requirements to verify that the machine has the required operating system patches and libraries.
  - Verify that the port numbers to use for application service processes are available on the machines where you install the Informatica services.
  - Review the distribution requirements to integrate the Informatica domain with the Hadoop or Databricks environment.
  - Verify that the operating system meets the file descriptor limit.
- ☐ Back up the Data Transformation files that were created in a previous installation.



- ☐ Review system environment variables.
- ☐ Create a system user account to run the installer.
- ☐ Set up keystore and truststore files if you want to configure secure communication for the domain and set up a secure connection to web client applications.
- ☐ Extract the installer files:
  - Verify installer code signing.
  - Verify installer package integrity with checksum.
- ☐ Verify the license key.

## Read the Release Notes

Read the Release Notes for updates to the installation and upgrade process. You can also find information about known and fixed issues for the release.

Find the Release Notes on the Informatica [documentation portal](#).

## Verify System Requirements

Verify that your environment meets the minimum system requirements for the installation process, temporary disk space, port availability, databases, and application service hardware.

For more information about product requirements and supported platforms, see the [Product Availability Matrix](#).

## Verify Temporary Disk Space and Permissions

Verify that your environment meets the minimum system requirements for the temporary disk space, permissions for the temporary files, and the Informatica client tools.

### **Disk space for the temporary files**

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

The following table describes the minimum disk space and memory requirements for PowerCenter or Data Engineering product installation:

Options	Minimum Requirements
Temporary disk space to run the installer	1 GB disk space
Install with application services for Data Engineering products	50 GB disk space, 8 GB RAM, and 8 cores. Out of the 50 GB, 25 GB is for the product installation binaries.
Install with application services for PowerCenter	50 GB disk space, 6 GB RAM, and 4 cores, Out of the 50 GB, 25 GB is for the product installation binaries.

#### Permissions for the temporary files

Verify that you have read, write, and execute permissions on the `/tmp` directory.

For more information about product requirements and supported platforms, see the [Product Availability Matrix](#).

## Review Patch Requirements on UNIX or Linux

Before you install the Informatica services, verify that the machine has the required operating system patches and libraries.

#### PowerCenter on UNIX

The following table lists the patches and libraries that the Informatica services require for PowerCenter on UNIX:

Platform	Compiler Version	Operating System	Operating System Patch
AIX	16	7.1 TL5	OS level: 7100-05 bos.adt.debug Version 7.1.5.32
AIX	16	7.2 TL4	OS level: 7200-04 bos.adt.debug Version 7.2.4.0

## PowerCenter on Linux

The following table lists the patches and libraries that the Informatica services require for PowerCenter on Linux:

Platform	Operating System	Operating System Patch
AWS Linux	Linux 2 - 2.0.20220805.0	All of the following packages: <ul style="list-style-type: none"><li>- e2fsprogs-libs-1.42.9-19.amzn2.x86_64</li><li>- keyutils-libs-1.5.8-3.amzn2.0.2.x86_64</li><li>- libsepol-2.5-8.1.amzn2.0.2.x86_64</li><li>- libselinux-2.5-12.amzn2.0.2.x86_64</li></ul>
Ubuntu	20.04.1	All of the following packages: <ul style="list-style-type: none"><li>- e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed]</li><li>- libkeyutils1/focal,now 1.6-6ubuntu1 amd64 [installed,automatic]</li><li>- libselinux1/focal,now 3.0-1build2 amd64 [installed,automatic]</li><li>- libsepol1/focal,now 3.0-1 amd64 [installed,automatic]</li></ul>
Ubuntu	18.04	All of the following packages: <ul style="list-style-type: none"><li>- e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed]</li><li>- libkeyutils1/focal,now 1.5.9-9.2ubuntu2 amd64 [installed,automatic]</li><li>- libselinux1/focal,now 2.7-2build2 amd64 [installed,automatic]</li><li>- libsepol1/focal,now 2.7-1ubuntu0.1 amd64 [installed,automatic]</li></ul>
Linux-x64	Red Hat Enterprise Linux 7.3	All of the following packages, where <version> is any version of the package: <ul style="list-style-type: none"><li>- e2fsprogs-libs-&lt;version&gt;.el7</li><li>- keyutils-libs-&lt;version&gt;.el7</li><li>- libselinux-&lt;version&gt;.el7</li><li>- libsepol-&lt;version&gt;.el7</li></ul>
Linux-x64	Red Hat Enterprise Linux 8	All of the following packages, where <version> is any version of the package: <ul style="list-style-type: none"><li>- e2fsprogs-libs-&lt;version&gt;.el8</li><li>- keyutils-libs-&lt;version&gt;.el8</li><li>- libselinux-&lt;version&gt;.el8</li><li>- libsepol-&lt;version&gt;.el8</li></ul>
Linux-x64	SUSE Linux Enterprise Server 12	Service Pack 2
Linux-x64	SUSE Linux Enterprise Server 15	Service Pack 0 and Service Pack 1.

## Verify Port Requirements

The installer sets up the ports for components in the Informatica domain, and it designates a range of dynamic ports to use for some application services.

You can specify the port numbers to use for the components and a range of dynamic port numbers to use for the application services. Or you can use the default port numbers provided by the installer. Verify that the port numbers are available on the machines where you run the installer.

**Note:** Services and nodes can fail to start if there is a port conflict.

The following table describes the port requirements for installation:

Port	Description
Node port	Port number for the node created during installation. Default is 6005.
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.
Range of dynamic ports for application services	Range of port numbers that can be dynamically assigned to application service processes as they start up. When you start an application service that uses a dynamic port, the Service Manager dynamically assigns the first available port in this range to the service process. The number of ports in the range must be at least twice the number of application service processes that run on the node. Default is 6014 to 6114. The Service Manager dynamically assigns port numbers from this range to the Model Repository Service.
Static ports for application services	Static ports have dedicated port numbers assigned that do not change. When you create the application service, you can accept the default port number, or you can manually assign the port number. The following services use static port numbers: <ul style="list-style-type: none"> <li>- Content Management Service. Default is 8105 for HTTP.</li> <li>- Data Integration Service. Default is 8095 for HTTP.</li> </ul>

## Guidelines for Port Configuration

The installer validates the port numbers that you specify to ensure that there will be no port conflicts in the domain.

Use the following guidelines to determine the port numbers:

- The port number you specify for the domain and for each component in the domain must be unique.
- The port number for the domain and domain components cannot be within the range of the port numbers that you specify for the application service processes.
- The highest number in the range of port numbers that you specify for the application service processes must be at least three numbers higher than the lowest port number. For example, if the minimum port number in the range is 6400, the maximum port number must be at least 6403.
- The port numbers that you specify cannot be lower than 1025 or higher than 65535.

## Verify Distribution Package Requirements (Linux and UNIX)

You can use third-party distribution packages to integrate the Informatica domain with the Hadoop or Databricks environment.

The Informatica domain and client require the distribution packages to process complex files within the Informatica domain or to connect to Hadoop or Databricks environment when you process within the Informatica domain.

If you need a distribution package, you can install it through the installer or through Integration Package Manager (the package manager) at any time.

You can use the Cloudera CDP Private Cloud distribution package to process complex files within the Informatica domain or to connect to the Hadoop or Databricks environment when you process within the Informatica domain. However, you can use a different distribution package according to your requirements.

The following adapters require distribution packages for processing within the Informatica domain:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Hadoop for PowerCenter
- PowerExchange for HBase
- PowerExchange for HDFS
- PowerExchange for Hive
- PowerExchange for JDBC V2
- PowerExchange for Kafka for PowerCenter
- PowerExchange for MapR-DB
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

## Verify the File Descriptor Limit

Verify that the operating system meets the file descriptor requirement.

Informatica service processes can use a large number of files. To prevent errors that result from the large number of files and processes, you can change system settings with the limit command if you use a C shell, or the ulimit command if you use a Bash shell.

### List Operating System Settings

To get a list of the operating system settings, including the file descriptor limit, run the following command:

With C shell, run `limit`

With Bash shell, run `ulimit -a`

### Set the File Descriptor Limit

Informatica service processes can use a large number of files. Set the file descriptor limit per process to 16,000 or higher. The recommended limit is 32,000 file descriptors per process.

To change system settings, run the limit or ulimit command with the pertinent flag and value. For example, to set the file descriptor limit, run the following command:

With C shell, run `limit -h filesize <value>`

With Bash shell, run `ulimit -n <value>`

## Set Max User Processes

Informatica services use a large number of user processes. Use the `ulimit -u` command to adjust the max user processes setting to a level that is high enough to account for all the processes required by the Blaze engine.

To set the max user processes, run the following command: Run the following command to set the max user processes setting:

With C shell, run `limit -u processes <value>`

With Bash shell, run `ulimit -u <value>`

## Verify Application Service Hardware Requirements

Verify that the nodes in the domain have adequate hardware for the Service Manager and the application services that run on the nodes.

You can create an Informatica domain with one node and run all application services on the same node. If you create an Informatica domain with multiple nodes, you can run the application services on separate nodes. When you plan the application services for the domain, consider system requirements based on the services that you run on a node.

**Note:** Based on workload and concurrency requirements, you might need to optimize performance by adding cores and memory on a node.

The following table lists the minimum system requirements for a node based on some common configuration scenarios. Use this information as a guideline for other configurations in your domain.

Services	Processor	Memory	Disk Space
One node runs the following services: <ul style="list-style-type: none"><li>- Analyst Service</li><li>- Content Management Service</li><li>- Data Integration Service</li><li>- Metadata Manager Service</li><li>- Model Repository Service</li><li>- PowerCenter Integration Service</li><li>- PowerCenter Repository Service</li><li>- Search Service</li><li>- Web Services Hub</li></ul>	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following services: <ul style="list-style-type: none"><li>- Analyst Service</li><li>- Content Management Service</li><li>- Data Integration Service</li><li>- Model Repository Service</li><li>- Search Service</li></ul>	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following service: <ul style="list-style-type: none"><li>- Analyst Service</li></ul>	1 CPU with multiple cores	4 GB	n/a
One node runs the following service: <ul style="list-style-type: none"><li>- Search Service</li></ul>	1 CPU with multiple cores	4 GB	10 GB

Services	Processor	Memory	Disk Space
One node runs the following services: - Analyst Service - Search Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Metadata Manager Service - PowerCenter Integration Service - PowerCenter Repository Service	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: - Metadata Manager Service - PowerCenter Integration Service - PowerCenter Repository Service	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: - PowerCenter Integration Service - PowerCenter Repository Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Data Integration Service - Model Repository Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Data Integration Service - Content Management Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following service: - Metadata Manager Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following service component: - Metadata Manager Agent	1 CPU with multiple cores	4 GB	400 MB
One node runs the following service: - Web Services Hub	1 CPU with multiple cores	4 GB	5 GB

## Back Up the Data Transformation Files

Before installation, you must back up the Data Transformation files that were created under previous versions. After you complete the installation, copy the files to the new installation directories to get the same repository and custom global components as in the previous version.

The following table lists the files or directories that you must back up:

File or Directory	Default Location
Repository	<Informatica installation directory>\DataTransformation\ServiceDB
Custom Global Components directory (TGP files)	<Informatica installation directory>\DataTransformation\autoInclude\user

File or Directory	Default Location
Custom Global Components directory (DLL and JAR files)	<Informatica installation directory>\DataTransformation\externLibs\user
Configuration file	<Informatica installation directory>\DataTransformation\CMConfig.xml
License file	<Informatica installation directory>\DataTransformation\CDELICENSE.cfg

Do not copy the Data Transformation Library files. Instead, install the Data Transformation Libraries again.

## Configure POSIX Asynchronous I/O

If you install Informatica on IBM AIX, make POSIX Asynchronous I/O available on any node where you want to run a PowerCenter Integration Service. A PowerCenter Integration Service running on an IBM AIX machine can fail to start if POSIX Asynchronous I/O is not available.

## Review the Environment Variables

Configure environment variables for the Informatica installation.

The following table describes the environment variables to review:

Variable	Description
IATEMPDIR	<p>Location of the temporary files created during installation. Informatica requires 1 GB disk space for temporary files.</p> <p>Configure the environment variable if you do not want to create temporary files in the /tmp directory.</p> <p>If you want to change the default /tmp directory, you must set IATEMPDIR and _JAVA_OPTIONS environment variables to the new directory.</p> <p>For example, set the variable to export IATEMPDIR=/home/user.</p> <p><b>Note:</b> Unset the IATEMPDIR variable after the installation.</p>
_JAVA_OPTIONS	<p>Configure the environment variable to change the temporary directory.</p> <p>If you want to change the default /tmp directory, you must set IATEMPDIR and _JAVA_OPTIONS the environment variables to the new directory.</p> <p>For example, set the variable to export _JAVA_OPTIONS=-Djava.io.tmpdir=/home/user.</p> <p><b>Note:</b> Unset the _JAVA_OPTIONS variable after the installation.</p>
LANG and LC_ALL	<p>Change the locale to set the appropriate character encoding for the terminal session. For example, set the encoding to <code>Latin1</code> or <code>ISO-8859-1</code> for French, <code>EUC-JP</code> or <code>Shift_JIS</code> for Japanese, or <code>UTF-8</code> for Chinese or Korean. The character encoding determines the types of characters that appear in the UNIX terminal.</p>



Variable	Description
DISPLAY	Unset the DISPLAY environment before you run the installer. Installation might fail if the DISPLAY environment variable has some value.
SKIP_VENDOR_CHECK	<p>Configure the environment variable to remove the sudo prompt from the installer on Linux or AIX.</p> <p>Set the environment variable to true to remove the sudo prompt from the Informatica server installation on Linux or AIX.</p> <p><b>Note:</b> If you don't have sudo privileges, set the environment variable to true before you run the installer. If you have sudo privileges, you don't need to set the environment variable.</p>

**Note:** Make sure that the NOEXEC flag is not set for the file system mounted on the /tmp directory.

## Create a System User Account

Create a user account specifically to run the Informatica service.

Verify that the user account you use to install Informatica has write permission on the installation directory.

Verify that the user account that installs the Informatica service does not have any privileges and permissions to access sensitive files on the machine where you install the Informatica services.

## Set Up a Keystore File

When you install the Informatica services, you can configure secure communication for the domain and set up a secure connection to Informatica Administrator (the Administrator tool). If you configure these security options, you must set up keystore and truststore files.

Before you install the Informatica services, set up the files for secure communication within the Informatica domain or for a secure connection to the Administrator tool. To create the required files, you can use the following programs:

### keytool

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

### OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website:

<https://www.openssl.org/docs/>

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or

implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

## Secure Communication Within the Informatica domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

### **You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

### **You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

### **You imported the certificate into keystores.**

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

**Note:** The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

### **You imported the certificate into truststores.**

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

### **The keystores and truststores are in the correct directory.**

The keystore and truststore must be in a directory that is accessible to the installer.

### **The keystore type used for the Administrator tool determines the keystore types for the Content Management Service.**

If you used the default keystore certificate for the Administrator tool, you can use either the default or a custom keystore certificate for the Content Management Service.

If you used a custom keystore certificate for the Administrator tool, you must use a custom keystore certificate for the Content Management Service.

For more information about how to create a custom keystore and truststore, see the [Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain"](#).

## Secure Connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

### **You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

### **You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

**The keystore is in the correct directory.**

The keystore must be in a directory that is accessible to the installer.

## Download and Extract the Installer Files

The installer files are distributed as compressed files. You can get the Informatica installation file and distribution packages from the FTP link contained in your fulfillment email.

Download the Informatica installation tar file and the required distribution package ZIP files from the Informatica Electronic Software Download site. You can download them to a local directory or a shared network drive that is mapped on your machine.

Extract the Informatica installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the executable file.

**Note:** Ensure that you extract the installer files to a local directory as you can't run the installer from a mapped file.

Copy the ZIP files of the distribution packages to the following location: `<Informatica installer files>/source`

**Note:** The installer fails if the ZIP files for distribution packages aren't available in the source directory.

## Verify Installer Code Signing

You can verify the signature of the Informatica software code.

Informatica uses a certificate based digital signature to sign the Informatica software code. The code signing helps to validate the authenticity of the code and ensures that there has been no changes or corruptions to the code after Informatica signs the code. You can determine whether to trust the software based on whether the code sign is present or not.

You can request a code signing certificate that contains information that fully identifies Informatica LLC and a Certificate Authority (CA) that issues the certificate. The digital certificate binds the identity of Informatica to a public key and to a private key.

Digital signing of software begins with the creation of a cryptographic hash, or a digest. The digest has a one to one correspondence with the original data. Use the digest as there are no hints on how to recreate the original data, and even a small change in the original data results in a change in the hash value. Informatica uses its private key to sign the digest, or generates a signature in the form of a string of bits. Good digital signature algorithms allow a user with the public key to verify the creator of the signature.

### To Verify the Signed Code is Authentic

After Informatica signs the software bundle, you can contact Informatica Global Customer Support to access the code signing certificate. Informatica ships the installer along with the signature file that contains the

hash of the installer binary encrypted with Informatica's private key. You can validate the integrity of digitally signed binaries using any available tools, such as OpenSSL.

For instance, if you have to verify the package authentication and confirm the code security, enter the following OpenSSL commands:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/
sign.sha256 <file>
```

Where **<signature>** is the file containing the signature in Base64, **<cert>** is the code signing certificate, and **<file>** is the file to verify.

Based on verification process, OpenSSL displays a success or error message to validate if the installer code is genuine or not. Note that the verification for the installer might take around two minutes.

## Verify Installer Package Checksum on UNIX and Linux

Before you run the services installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installers.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

The following table lists the checksum and file size for the Informatica services installer for UNIX and Linux:

File	Checksum Value	File Size
informatica_1053_server_linux-x64.tar	2154528627	11639828480
informatica_1053_server_aix-ppc64.tar	561493064	10006200320

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see

[HOW TO: Identify file errors after downloading Informatica installation files.](#)

## Verify the License Key

Before you install the software, verify that you have the license key available.

When you download the installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have a license key or if you have an incremental license key and you want to create a domain.

## CHAPTER 3

# Before You Install the Services on Windows

This chapter includes the following topics:

- [Before You Install the Services on Windows Overview, 37](#)
- [Read the Release Notes, 37](#)
- [Verify System Requirements, 38](#)
- [Back Up the Data Transformation Files, 42](#)
- [Review the Environment Variables, 42](#)
- [Create a System User Account, 43](#)
- [Set Up Keystore and Truststore Files, 43](#)
- [Download and Extract the Installer Files, 45](#)
- [Verify the License Key, 46](#)

## Before You Install the Services on Windows Overview

Before you install the Informatica services, set up the machine to meet the requirements to install and run the Informatica platform. If the machine where you install the Informatica services is not configured correctly, the installation can fail.

## Read the Release Notes

Read the Release Notes for updates to the installation and upgrade process. You can also find information about known and fixed issues for the release.

Find the Release Notes on the Informatica [documentation portal](#).

# Verify System Requirements

Verify that your environment meets the minimum system requirements for the installation process, temporary disk space, port availability, databases, and application service hardware.

For more information about product requirements and supported platforms, see the [Product Availability Matrix](#).

## Verify Temporary Disk Space and Permissions

Verify that your environment meets the minimum system requirements for the temporary disk space, permissions for the temporary files, and the Informatica client tools.

### Disk space for the temporary files

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

The following table describes the minimum disk space and memory requirements for PowerCenter or Data Engineering product installation:

Options	Minimum Requirements
Temporary disk space to run the installer	1 GB disk space
Install with application services for Data Engineering products	50 GB disk space, 8 GB RAM, and 8 cores. Out of the 50 GB, 25 GB is for the product installation binaries.
Install with application services for PowerCenter	50 GB disk space, 6 GB RAM, and 4 cores, Out of the 50 GB, 25 GB is for the product installation binaries.

### Permissions for the temporary files

Verify that you have read, write, and execute permissions on the `/tmp` directory.

For more information about product requirements and supported platforms, see the [Product Availability Matrix](#).

## Review the Patch Requirements

Before you install the Informatica services, verify that the machine has the required operating system patches and libraries.

The following table lists the patches and libraries that the Informatica services require on a Windows platform:

Platform	Operating System	Operating System Patch
Windows x64	2016 64-bit	None required
Windows 2019	2019 64-bit	None required
Windows 2022	2022 64-bit	None required

## Verify Port Requirements

The installer sets up the ports for components in the Informatica domain, and it designates a range of dynamic ports to use for some application services.

You can specify the port numbers to use for the components and a range of dynamic port numbers to use for the application services. Or you can use the default port numbers provided by the installer. Verify that the port numbers are available on the machines where you run the installer.

**Note:** Services and nodes can fail to start if there is a port conflict.

The following table describes the port requirements for installation:

Port	Description
Node port	Port number for the node created during installation. Default is 6005.
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.
Range of dynamic ports for application services	Range of port numbers that can be dynamically assigned to application service processes as they start up. When you start an application service that uses a dynamic port, the Service Manager dynamically assigns the first available port in this range to the service process. The number of ports in the range must be at least twice the number of application service processes that run on the node. Default is 6014 to 6114.  The Service Manager dynamically assigns port numbers from this range to the Model Repository Service.
Static ports for application services	Static ports have dedicated port numbers assigned that do not change. When you create the application service, you can accept the default port number, or you can manually assign the port number.  The following services use static port numbers: <ul style="list-style-type: none"><li>- Content Management Service. Default is 8105 for HTTP.</li><li>- Data Integration Service. Default is 8095 for HTTP.</li></ul>

## Guidelines for Port Configuration

The installer validates the port numbers that you specify to ensure that there will be no port conflicts in the domain.

Use the following guidelines to determine the port numbers:

- The port number you specify for the domain and for each component in the domain must be unique.
- The port number for the domain and domain components cannot be within the range of the port numbers that you specify for the application service processes.
- The highest number in the range of port numbers that you specify for the application service processes must be at least three numbers higher than the lowest port number. For example, if the minimum port number in the range is 6400, the maximum port number must be at least 6403.
- The port numbers that you specify cannot be lower than 1025 or higher than 65535.

## Verify Distribution Package Requirements (Windows)

The Informatica domain and client require the distribution packages to process complex files within the domain or to connect to Hadoop or Databricks environment when you process within the domain.

If you need a distribution package, you can install it through the installer or through Integration Package Manager (the package manager) at any time.

You can use the Cloudera CDP Private Cloud distribution package to process complex files within the Informatica domain or to connect to the Hadoop or Databricks environment when you process within the Informatica domain. However, you can use a different distribution package according to your requirements.

The following adapters require distribution packages for processing within the Informatica domain:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Kafka for PowerCenter
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

## Verify Application Service Hardware Requirements

Verify that the nodes in the domain have adequate hardware for the Service Manager and the application services that run on the nodes.

You can create an Informatica domain with one node and run all application services on the same node. If you create an Informatica domain with multiple nodes, you can run the application services on separate nodes. When you plan the application services for the domain, consider system requirements based on the services that you run on a node.

**Note:** Based on workload and concurrency requirements, you might need to optimize performance by adding cores and memory on a node.



The following table lists the minimum system requirements for a node based on some common configuration scenarios. Use this information as a guideline for other configurations in your domain.

Services	Processor	Memory	Disk Space
One node runs the following services: <ul style="list-style-type: none"> <li>- Analyst Service</li> <li>- Content Management Service</li> <li>- Data Integration Service</li> <li>- Metadata Manager Service</li> <li>- Model Repository Service</li> <li>- PowerCenter Integration Service</li> <li>- PowerCenter Repository Service</li> <li>- Search Service</li> <li>- Web Services Hub</li> </ul>	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Analyst Service</li> <li>- Content Management Service</li> <li>- Data Integration Service</li> <li>- Model Repository Service</li> <li>- Search Service</li> </ul>	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following service: <ul style="list-style-type: none"> <li>- Analyst Service</li> </ul>	1 CPU with multiple cores	4 GB	n/a
One node runs the following service: <ul style="list-style-type: none"> <li>- Search Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Analyst Service</li> <li>- Search Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Metadata Manager Service</li> <li>- PowerCenter Integration Service</li> <li>- PowerCenter Repository Service</li> </ul>	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Metadata Manager Service</li> <li>- PowerCenter Integration Service</li> <li>- PowerCenter Repository Service</li> </ul>	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- PowerCenter Integration Service</li> <li>- PowerCenter Repository Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Data Integration Service</li> <li>- Model Repository Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: <ul style="list-style-type: none"> <li>- Data Integration Service</li> <li>- Content Management Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB
One node runs the following service: <ul style="list-style-type: none"> <li>- Metadata Manager Service</li> </ul>	1 CPU with multiple cores	4 GB	10 GB

Services	Processor	Memory	Disk Space
One node runs the following service component: - Metadata Manager Agent	1 CPU with multiple cores	4 GB	400 MB
One node runs the following service: - Web Services Hub	1 CPU with multiple cores	4 GB	5 GB

## Back Up the Data Transformation Files

Before installation, you must back up the Data Transformation files that were created under previous versions. After you complete the installation, copy the files to the new installation directories to get the same repository and custom global components as in the previous version.

The following table lists the files or directories that you must back up:

File or Directory	Default Location
Repository	<Informatica installation directory>\DataTransformation\ServiceDB
Custom Global Components directory (TGP files)	<Informatica installation directory>\DataTransformation\autoInclude\user
Custom Global Components directory (DLL and JAR files)	<Informatica installation directory>\DataTransformation\externLibs\user
Configuration file	<Informatica installation directory>\DataTransformation\CMConfig.xml
License file	<Informatica installation directory>\DataTransformation\CDELICENSE.cfg

Do not copy the Data Transformation Library files. Instead, install the Data Transformation Libraries again.

## Review the Environment Variables

Configure the environment variables to work with the Informatica installation.

The following table describes environment variables to review on Windows:

Variable	Description
%TEMP%	Location of the temporary files created during installation. Informatica requires 1 GB disk space for temporary files. Configure the environment variable if you do not want to create temporary files in the default drive.
PATH	The installer appends file paths required by Informatica to the PATH environment variable. Verify that the length of the PATH environment variable does not exceed the system limits.

## Create a System User Account

Create a system user account to perform the installation and to run the Informatica service. Verify that the user account that you use to install the Informatica services has write permission on the installation directory.

You can install Informatica with the user account logged in to the machine and run it under another user account. You can create a local account or a domain account to install Informatica or run the Informatica Windows service.

**Note:** To access a repository on Microsoft SQL Server that uses a Windows trusted connection, create a domain account.

The user accounts require the following permissions to run the installer or to run the Informatica Windows service:

- **Logged in user account.** The user account must be a member of the Administrators group and have the *Log on as a service* permission. Log in with this user account before you install Informatica.
- **Another user account.** The user account must be a member of the Administrators group and have Log on as a service and Act as operating system permissions. You do not have to log in with this user account before you install Informatica. During installation, you can specify the user account to run the Informatica Windows service.

## Set Up Keystore and Truststore Files

When you install the Informatica services, you can configure secure communication for the domain and set up a secure connection to Informatica Administrator (the Administrator tool). If you configure these security options, you must set up keystore and truststore files.

Before you install the Informatica services, set up the files for secure communication within the Informatica domain or for a secure connection to the Administrator tool. To create the required files, you can use the following programs:

### **keytool**

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

For more information about using keytool, see the documentation on the following web site:

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>.

## OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website:

<https://www.openssl.org/docs/>

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

## Secure Communication Within the Informatica domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

### **You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

### **You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

### **You imported the certificate into keystores.**

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

**Note:** The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

### **You imported the certificate into truststores.**

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

### **The keystores and truststores are in the correct directory.**

The keystore and truststore must be in a directory that is accessible to the installer.

## Secure Connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

### **You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

### **You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

**The keystore is in the correct directory.**

The keystore must be in a directory that is accessible to the installer.

## Download and Extract the Installer Files

The installer files are distributed as compressed files. You can get the Informatica installation file and distribution packages from the FTP link contained in your fulfillment email.

Download the Informatica installation tar file and the required distribution package ZIP files from the Informatica Electronic Software Download site. You can download them to a local directory or a shared network drive that is mapped on your machine.

Extract the Informatica installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the executable file.

**Note:** Ensure that you extract the installer files to a local directory as you can't run the installer from a mapped file.

Copy the ZIP files of the distribution packages to the following location: `<Informatica installer files>/source`

**Note:** The installer fails if the ZIP files for distribution packages aren't available in the source directory.

## Verify Installer Code Signing

You can verify the signature of the Informatica software code.

Informatica uses a certificate based digital signature to sign the Informatica software code. The code signing helps to validate the authenticity of the code and ensures that there has been no changes or corruptions to the code after Informatica signs the code. You can determine whether to trust the software based on whether the code sign is present or not.

You can request a code signing certificate that contains information that fully identifies Informatica LLC and a Certificate Authority (CA) that issues the certificate. The digital certificate binds the identity of Informatica to a public key and to a private key.

Digital signing of software begins with the creation of a cryptographic hash, or a digest. The digest has a one to one correspondence with the original data. Use the digest as there are no hints on how to recreate the original data, and even a small change in the original data results in a change in the hash value. Informatica uses its private key to sign the digest, or generates a signature in the form of a string of bits. Good digital signature algorithms allow a user with the public key to verify the creator of the signature.

### To Verify the Signed Code is Authentic

After Informatica signs the software bundle, you can contact Informatica Global Customer Support to access the code signing certificate. Informatica ships the installer along with the signature file that contains the

hash of the installer binary encrypted with Informatica's private key. You can validate the integrity of digitally signed binaries using any available tools, such as OpenSSL.

For instance, if you have to verify the package authentication and confirm the code security, enter the following OpenSSL commands:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/
sign.sha256 <file>
```

Where **<signature>** is the file containing the signature in Base64, **<cert>** is the code signing certificate, and **<file>** is the file to verify.

Based on verification process, OpenSSL displays a success or error message to validate if the installer code is genuine or not. Note that the verification for the installer might take around two minutes.

## Verify Installer Package Checksum on Windows

Before you run the services installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installer.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

The following table lists the checksum and file size for Informatica services on Windows:

File	Checksum Value	File Size
informatica_1053_server_winem-64t.zip	3333101514	10112422360

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see [HOW TO: Identify file errors after downloading Informatica installation files](#).

## Verify the License Key

Before you install the software, verify that you have the license key available.

When you download the installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have a license key or if you have an incremental license key and you want to create a domain.

## CHAPTER 4

# Prepare for Application Services and Databases

This chapter includes the following topics:

- [Checklist to Prepare for Application Services , 47](#)
- [Prepare for Application Services and Databases Overview, 48](#)
- [Set Up Database User Accounts, 48](#)
- [Identify Application Services by Product, 48](#)
- [Domain Configuration Repository Database Requirements, 49](#)
- [Analyst Service , 53](#)
- [Content Management Service, 54](#)
- [Data Integration Service, 56](#)
- [Metadata Manager Service, 62](#)
- [Model Repository Service, 67](#)
- [Monitoring Model Repository Service, 71](#)
- [PowerCenter Integration Service, 71](#)
- [PowerCenter Repository Service, 72](#)
- [Search Service, 75](#)
- [Configure Native Connectivity on Service Machines, 76](#)

## Checklist to Prepare for Application Services

This chapter contains information about application services and databases for the Informatica environment. Use this checklist to track service planning and database preparation.

- ☐ Identify the application services that you need in your environment.
- ☐ Identify the application services that you want the installer to create.
- ☐ Prepare databases for the services:
  - Create the database.
  - Create a user for the database.
  - Create environment variables.

- Configure connectivity.

## Prepare for Application Services and Databases Overview

When you plan the application services, you must account for the associated services that connect to the application service. You also must plan the relational databases that the application service requires.

The installer prompts you to optionally create some services during the installation. Some service properties require database information. If you want the installer to create a service that requires a database, you must prepare the database before you run the installer. To prepare the databases, verify the data base requirements, set up the database, and set up a user account. The database requirements depend on the application services that you create.

If you do not create services during installation, you can create them manually after you install.

## Set Up Database User Accounts

Set up a database and user account for the repository databases.

Use the following rules and guidelines when you set up the user accounts:

- The database user account must have permissions to create and drop tables, indexes, and views, and to select, insert, update, and delete data from tables.
- Use 7-bit ASCII to create the password for the account.
- To prevent database errors in one repository from affecting any other repository, create each repository in a separate database schema with a different database user account. Do not create a repository in the same database schema as the domain configuration repository or any other repository in the domain.

## Identify Application Services by Product

Each application service provides different functionality within the Informatica domain. You create application services based on the license key generated for your organization.



The following table lists the application services that the PowerCenter and Informatica Data Quality products use:

Product	Application Services
PowerCenter	<ul style="list-style-type: none"> <li>- Analyst Service</li> <li>- Content Management Service *</li> <li>- Data Integration Service *</li> <li>- Metadata Manager Service</li> <li>- Model Repository Service *</li> <li>- monitoring Model Repository Service *</li> <li>- PowerCenter Integration Service *</li> <li>- PowerCenter Repository Service *</li> <li>- Search Service</li> <li>- Web Services Hub Service</li> </ul>
Informatica Data Quality	<ul style="list-style-type: none"> <li>- Analyst Service</li> <li>- Content Management Service *</li> <li>- Data Integration Service *</li> <li>- Metadata Manager Service</li> <li>- Model Repository Service *</li> <li>- monitoring Model Repository Service *</li> <li>- PowerCenter Integration Service *</li> <li>- PowerCenter Repository Service *</li> <li>- Search Service</li> </ul>
<p><i>* You can create these services when you install the product.</i></p> <p><i>Note that services might vary depending on the product edition you have.</i></p>	

## Domain Configuration Repository Database Requirements

Informatica components store metadata in relational database repositories. The domain stores configuration and user information in a domain configuration repository.

You must set up a database and user account for the domain configuration repository before you run the installation. The database must be accessible to all gateway nodes in the Informatica domain.

When you install Informatica, you provide the database and user account information for the domain configuration repository. The Informatica installer uses JDBC to communicate with the domain configuration repository.

The domain configuration repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL
- Sybase ASE

Allow 200 MB of disk space for the database.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2\_SKIPINSERTED
  - DB2\_EVALUNCOMMITTED
  - DB2\_SKIPDELETED
  - AUTO\_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a non-partitioned tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the open\_cursors parameter to 4000 or higher.
- Set the permissions on the view \$parameter for the database user.
- Set the privileges for the database user to run *show parameter open\_cursors* in the Oracle database. When you run the pre-installation (i10Pi) system check tool, i10Pi runs the command against the database to identify the OPEN\_CURSORS parameter with the domain database user credentials.

You can run the following query to determine the open cursors setting for the domain database user account:

```
SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
```

- Verify that the database user has the following privileges:

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE SYNONYM
```

```
CREATE TABLE
```

```
CREATE VIEW
```

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## PostgreSQL Database Requirements

Use the following guidelines when you set up the repository on PostgreSQL:

- Verify that the database user account has CONNECT, CREATE TABLE, and CREATE VIEW privileges.
- Specify the database schema name when you use PostgreSQL as the database.
- Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

`<PostgreSQL installation directory>/data`

- On the database, set the configuration parameters.

The following table lists the minimum and recommended values for the configuration parameters that you must set:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

## Sybase Database Requirements

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 16K or higher. You must set the page size to 16K as this is a one-time configuration and cannot be changed afterwards.
- Set the database locking configuration to use row-level locking.

The following table describes the database locking configuration that you must set:

Database Configuration	Sybase System Procedure	Value
Lock scheme	sp_configure "lock scheme"	0, datarows

- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Turn ON the Sybase database option select into/bulkcopy/pllsort.
- Enable the "select" privilege for the sysobjects system table.
- Create the following login script to disable the default VARCHAR truncation:

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

The login script is executed every time the user logs into the Sybase instance. The stored procedure sets the parameter at the session level. The sp\_modifylogin system procedure updates "user\_name" with the stored procedure as its "login script". The user must have permission to invoke the stored procedure.

- Verify that the database user has CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, and CREATE VIEW privileges.
- Set the database configurations to the recommended baseline values.  
The following table lists the database memory configuration parameters that you must set:

Database Configuration	Sybase System Procedure	Value
Maximum amount of total physical memory	sp_configure "max memory"	2097151
Procedure cache size	sp_configure "procedure cache size"	500000
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	5000
Heap memory per user	sp_configure "heap memory per user"	49152
Number of locks	sp_configure "number of locks"	100000

## Analyst Service

The Analyst service runs the Analyst tool. It manages the connections between service components and the user that have access to the Analyst tool. When you create the service, you need to associate other application services with it.

The following table summarizes some dependencies that are associated with the Analyst Service:

Dependency	Summary
Products	The following products use the Analyst Service: <ul style="list-style-type: none"> <li>- Data Engineering Integration</li> <li>- Data Engineering Quality</li> <li>- Data Engineering Streaming</li> <li>- Enterprise Data Catalog</li> <li>- Informatica Data Quality</li> <li>- PowerCenter</li> <li>- Test Data Management</li> </ul>
Services	The Analyst Service requires a direct association with the following services: <ul style="list-style-type: none"> <li>- Data Integration Service</li> <li>- Model Repository Service</li> </ul>
Databases	The Analyst Service does not have any associated database.
Installer	You cannot create the Analyst Service during installation.

# Content Management Service

The Content Management Service manages reference data for data domains that use reference tables. It uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. When you create the service, you need to associate other application services with it.

The following table summarizes the dependencies for products, services, and databases that are associated with the Content Management Service:

Dependency	Summary
Products	The following products use the Content Management Service: <ul style="list-style-type: none"><li>- Data Engineering Quality</li><li>- Data Privacy Management</li><li>- Enterprise Data Catalog</li><li>- Enterprise Data Preparation</li><li>- Informatica Data Quality</li><li>- Test Data Management</li></ul>
Services	The Content Management Service requires a direct association with the following services: <ul style="list-style-type: none"><li>- Model Repository Service</li><li>- Data Integration Service</li></ul>
Databases	The Content Management Service uses the following database: <ul style="list-style-type: none"><li>- Reference data warehouse. Stores data values for the reference table objects that you define in the Model repository. When you add data to a reference table, the Content Management Service writes the data values to a table in the reference data warehouse.</li></ul>
Installer	You can create the Content Management Service when you run the installer. <b>Note:</b> You must create the Content Management Service on the same node as the Data Integration Service.

## Reference Data Warehouse Requirements

The reference data warehouse stores the data values for reference table objects that you define in a Model repository. You configure a Content Management Service to identify the reference data warehouse and the Model repository.

You associate a reference data warehouse with a single Model repository. You can select a common reference data warehouse on multiple Content Management Services if the Content Management Services identify a common Model repository. The reference data warehouse must support mixed-case column names.

The reference data warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL, using a JDBC driver

Allow 200 MB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the Content Management Service.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Verify that the database user has SELECT privileges on the SYSCAT.DBAUTH and SYSCAT.DBTABAUTH tables.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

## Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

ALTER SEQUENCE

ALTER TABLE

CREATE SEQUENCE

CREATE SESSION

CREATE TABLE

CREATE VIEW

DROP SEQUENCE

DROP TABLE

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## PostgreSQL Database Requirements

Use the following guidelines when you set up the repository on PostgreSQL:

- Use a JDBC connection to connect to the PostgreSQL database.  
Informatica installs a DataDirect JDBC driver for PostgreSQL that you can use to connect to the database. Find the driver in the clients/DeveloperClient/infacmd installation directory, and copy the driver to the clients/externaljdbcjars directory .
- Specify the database schema name. Do not leave the schema name blank.  
If the database uses the default PostgreSQL schema name of `public`, you can specify `public` as the schema name.
- Verify that the database user has the `CONNECT` and `CREATE TABLE` privileges.

## Data Integration Service

The Data Integration Service receives requests from Informatica client tools to run integration, profile, and data preparation jobs. It writes results to different databases, and it writes run-time metadata to the Model repository. When you create the service, you need to associate another application service with it.

The following table lists the dependencies for products, services, and databases that are associated with the Data Integration Service.

Dependency	Summary
Products	The following products use the Data Integration Service: <ul style="list-style-type: none"><li>- Data Engineering Integration</li><li>- Data Engineering Quality</li><li>- Data Engineering Streaming</li><li>- Data Privacy Management</li><li>- Enterprise Data Catalog</li><li>- Enterprise Data Preparation</li><li>- Informatica Data Quality</li><li>- PowerCenter</li><li>- Test Data Management</li></ul>
Services	The Data Integration Service requires a direct association with the following service: <ul style="list-style-type: none"><li>- Model Repository Service</li></ul>
Databases	The Data Integration Service uses the following databases: <ul style="list-style-type: none"><li>- Data object cache. Stores cached logical data objects and virtual tables.</li><li>- Profiling warehouse. Stores profiling information, such as profile and scorecard results.</li><li>- Workflow database. Stores run-time metadata for workflows.</li></ul>
Installer	You can create the Data Integration Service when you run the installer.



## Data Object Cache Database Requirements

The data object cache database stores cached logical data objects and virtual tables for the Data Integration Service. You specify the data object cache database connection when you create the Data Integration Service.

The data object cache database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 200 MB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the Data Integration Service.

### IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

### Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

### Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
  - CREATE INDEX
  - CREATE SESSION
  - CREATE SYNONYM
  - CREATE TABLE
  - CREATE VIEW
  - DROP TABLE
  - INSERT INTO TABLE
  - UPDATE TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## Profiling Warehouse Requirements

The profiling warehouse database stores profiling and scorecard results. You specify the profiling warehouse connection when you create the Data Integration Service.

The profiling warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Allow 10 GB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the Data Integration Service. You can specify a JDBC connection as the profiling warehouse connection for IBM DB2 UDB, Microsoft SQL Server, and Oracle database types.

For more information about configuring the database, see the documentation for your database system.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- The database user account must have the CREATETAB, CONNECT, CREATE VIEW, and CREATE FUNCTION privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

**Note:** Informatica does not support the partitioned database environment for IBM DB2 databases when you use a JDBC connection as the profiling warehouse connection.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- The database user account must have the CONNECT, CREATE TABLE, CREATE VIEW, and CREATE FUNCTION privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
  - ALTER TABLE
  - CREATE ANY INDEX
  - CREATE PROCEDURE
  - CREATE SESSION
  - CREATE TABLE
  - CREATE VIEW
  - DROP TABLE
  - UPDATE TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the following parameters to the Informatica recommended values:

Parameter	Recommended Value
open_cursors	4000
Sessions	1000
Processes	1000

## Workflow Database Requirements

The Data Integration Service stores run-time metadata for workflows in the workflow database. Before you create the workflow database, set up a database and database user account for the workflow database.

You specify the workflow database connection when you create the Data Integration Service.

The workflow database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

Allow 200 MB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the Data Integration Service.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Set the connection pooling parameters.

The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

## Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.
- Set the connection pooling parameters.

The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
  - ALTER TABLE
  - ALTER VIEW
  - CREATE SEQUENCE
  - CREATE SESSION
  - CREATE SYNONYM
  - CREATE TABLE
  - CREATE VIEW
  - DROP TABLE
  - DROP VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the connection pooling parameters.

The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

## PostgreSQL Database Requirements

Use the following guidelines when you set up the repository on PostgreSQL:

- Use a JDBC connection to connect to the PostgreSQL database.
- Verify that the database user account has CONNECT, CREATE TABLE, and CREATE VIEW privileges.
- Specify the database schema name when you use PostgreSQL as the database.
- Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

`<PostgreSQL installation directory>/data`

- On the database, set the configuration parameters.

The following table lists the minimum and recommended values for the configuration parameters that you must set:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

## Metadata Manager Service

The Metadata Manager Service runs the Metadata Manager web client in the Informatica domain. The Metadata Manager Service manages the connections between service components and the users that have access to Metadata Manager.

The following table summarizes the dependencies for products, services, and databases that are associated with the Metadata Manager Service.

Dependency	Summary
Products	The following products use the Metadata Manager Service: <ul style="list-style-type: none"> <li>- Informatica Data Quality</li> <li>- PowerCenter</li> </ul>
Services	The Metadata Manager Service requires a direct association with the following services: <ul style="list-style-type: none"> <li>- PowerCenter Integration Service</li> <li>- PowerCenter Repository Service</li> </ul>
Databases	The Metadata Manager Service uses the following database: <ul style="list-style-type: none"> <li>- Metadata Manager repository. Stores the Metadata Manager warehouse and metadata models.</li> </ul>
Installer	You cannot create the Metadata Manager Service when you run the installer. You must create the service after the installation completes.

## Metadata Manager Repository Database Requirements

The Metadata Manager repository is a centralized location in a relational database that stores metadata from disparate metadata sources. It also stores the Metadata Manager warehouse and the models for each metadata source type. Each Metadata Manager application is configured to run with one Metadata Manager repository.

The Metadata Manager repository supports the following database types:

- IBM DB2 UDB

- Microsoft SQL Server
- Oracle

Allow 1 GB of disk space for the database.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- The database user account that creates the repository must have privileges to perform the following operations:
  - ALTER TABLE
  - CREATE FUNCTION
  - CREATE INDEX
  - CREATE PROCEDURE
  - CREATE TABLE
  - CREATE VIEW
  - DROP PROCEDURE
  - DROP TABLE
  - INSERT INTO
- The database user that creates the repository must be able to create tablespaces with page sizes of 32 KB.
- Set up system temporary tablespaces larger than the default page size of 4 KB and update the heap sizes. Queries running against tables in tablespaces defined with a page size larger than 4 KB require system temporary tablespaces with a page size larger than 4 KB. If there are no system temporary table spaces defined with a larger page size, the queries can fail. The server displays the following error:

```
SQL 1585N A system temporary table space with sufficient page size does not exist.
SQLSTATE=54048
```

Create system temporary tablespaces with page sizes of 8 KB, 16 KB, and 32 KB. Run the following SQL statements on each database to configure the system temporary tablespaces and update the heap sizes:

```
CREATE Bufferpool RBF IMMEDIATE  SIZE 1000 PAGESIZE 32 K  EXTENDED STORAGE ;
CREATE Bufferpool STBF IMMEDIATE  SIZE 2000 PAGESIZE 32 K  EXTENDED STORAGE ;
CREATE REGULAR  TABLESPACE REGTS32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING
('C:\DB2\NODE0000\reg32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE
0.33 BUFFERPOOL RBF;
CREATE SYSTEM TEMPORARY  TABLESPACE TEMP32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING
('C:\DB2\NODE0000\temp32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE
0.33 BUFFERPOOL STBF;
GRANT USE OF TABLESPACE REGTS32 TO USER <USERNAME>;
UPDATE DB CFG FOR <DB NAME> USING APP_CTL_HEAP_SZ 16384
UPDATE DB CFG FOR <DB NAME> USING APPLHEAPSZ 16384
UPDATE DBM CFG USING QUERY_HEAP_SZ 8000
UPDATE DB CFG FOR <DB NAME> USING LOGPRIMARY 100
UPDATE DB CFG FOR <DB NAME> USING LOGFILSIZ 2000
UPDATE DB CFG FOR <DB NAME> USING LOCKLIST 1000
UPDATE DB CFG FOR <DB NAME> USING DBHEAP 2400
"FORCE APPLICATIONS ALL"
DB2STOP
DB2START
```

- Set the locking parameters to avoid deadlocks when you load metadata into a Metadata Manager repository on IBM DB2.

The following table lists the locking parameters you can configure:

Parameter Name	Value	IBM DB2 Description
LOCKLIST	8192	Max storage for lock list (4KB)
MAXLOCKS	10	Percent of lock lists per application
LOCKTIMEOUT	300	Lock timeout (sec)
DLCHKTIME	10000	Interval for checking deadlock (ms)

Also, for IBM DB2 9.7 and earlier, set the DB2\_RR\_TO\_RS parameter to YES to change the read policy from Repeatable Read to Read Stability.

- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

**Note:** If you use IBM DB2 as a metadata source, the source database has the same configuration requirements.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- The database user account that creates the repository must have privileges to perform the following operations:
  - ALTER TABLE
  - CREATE CLUSTERED INDEX
  - CREATE INDEX
  - CREATE PROCEDURE
  - CREATE TABLE
  - CREATE VIEW
  - DROP PROCEDURE
  - DROP TABLE
  - INSERT INTO
- If the repository must store metadata in a multibyte language, set the database collation to that multibyte language when you install Microsoft SQL Server. For example, if the repository must store metadata in Japanese, set the database collation to a Japanese collation when you install Microsoft SQL Server. This is a one-time configuration and cannot be changed.



## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

- ALTER TABLE
  - CREATE CLUSTER
  - CREATE INDEX
  - CREATE OR REPLACE FORCE VIEW
  - CREATE OR REPLACE PROCEDURE
  - CREATE OR REPLACE VIEW
  - CREATE SESSION
  - CREATE TABLE
  - DROP TABLE
  - INSERT INTO TABLE

- Set the following parameters for the tablespace on Oracle:

### **<Temporary tablespace>**

Resize to at least 2 GB.

### **CURSOR\_SHARING**

Set to FORCE.

### **MEMORY\_TARGET**

Set to at least 4 GB.

Run `SELECT * FROM v$memory_target_advice ORDER BY memory_size;` to determine the optimal MEMORY\_SIZE.

### **MEMORY\_MAX\_TARGET**

Set to greater than the MEMORY\_TARGET size.

If MEMORY\_MAX\_TARGET is not specified, MEMORY\_MAX\_TARGET defaults to the MEMORY\_TARGET setting.

### **OPEN\_CURSORS**

Set to 3000 shared.

Monitor and tune open cursors. Query `v$sesstat` to determine the number of currently-opened cursors. If the sessions are running close to the limit, increase the value of OPEN\_CURSORS.

### **UNDO\_MANAGEMENT**

Set to AUTO.

- If the repository must store metadata in a multibyte language, set the NLS\_LENGTH\_SEMANTICS parameter to CHAR on the database instance. Default is BYTE.
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## Split Domain for Metadata Manager

If your product bundle includes Metadata Manager, you must decide whether to create one domain or a split domain. In a split domain, the application services associated with the primary components of your product

bundle run in one domain, and the application services associated with Metadata Manager run in a separate domain.

When you configure a split domain, you can upgrade Metadata Manager without having to upgrade the primary components of your product bundle. Metadata Manager can run on a more recent product version than the other components.

For example, your product bundle includes PowerCenter and Metadata Manager. In a split domain, the application services associated with PowerCenter run in the primary domain, while the application services associated with Metadata Manager run in the secondary domain. To upgrade Metadata Manager, you upgrade the product components in the secondary domain. You can upgrade Metadata Manager without having to upgrade PowerCenter at the same time.

To create each domain, you run the Informatica services installer separately. You can create each domain on a separate machine or you can create both domains on one machine.

## Split Domain Considerations

Before you decide to create a split domain, consider the advantages and potential issues.

The primary advantage of a split domain is that it supports frequent upgrades for Metadata Manager. You can upgrade Metadata Manager without having to upgrade other components of your product bundle at the same time. Therefore, you can take advantage of Metadata Manager new features and bug fixes without affecting activities in the primary domain such as data integration operations. The primary domain remains fully operational while you upgrade Metadata Manager.

However, you should also consider the following issues:

### **A split domain configuration is more complex than a single domain configuration.**

In a split domain, you must create duplicate services, repositories, and users. If you install both domains on the same machine, you must ensure that there are no port conflicts for the components in each domain. When you run different Informatica versions in each domain, you must also consider possible database version conflicts. For example, you create PowerCenter repositories for different Informatica product versions in the same Oracle database. You must ensure that both Informatica product versions support the Oracle database version.

### **There might be license implications.**

If you use Informatica products for data integration, your license agreement usually limits data integration activities to one domain. Your license agreement might limit the number of machines on which you can create application services or the types of services that you can duplicate. You might also need a separate license file for each domain.

For questions about licensing, contact your Informatica products representative.

### **You need additional database schemas and user accounts.**

In a split domain, you must create duplicate repositories. For example, you create a domain configuration repository in each domain. If you run PowerCenter and Metadata Manager in separate domains, you also create a PowerCenter repository in each domain.

Each repository must be in a separate schema. You also need a separate database user account for each domain configuration repository.

### **You need additional RAM and disk space.**

When you install Informatica services, the amount of required RAM and disk space for two domains is twice the required amount for one domain.

**There are product version restrictions.**

In a split domain, the components in the secondary domain can run the same version or a later version of Informatica products than the components in the primary domain. Therefore, you can run a later version of Metadata Manager than PowerCenter. However, you cannot run a later version of PowerCenter than Metadata Manager.

**You might need to run a different version of the PowerCenter Client in each domain.**

For example, you run the PowerCenter Client in the primary domain to perform data integration operations. In the secondary domain, you run a later version of Metadata Manager. To view session logs from Metadata Manager resource loads, you must run a later version of the PowerCenter Client in the secondary domain.

**You cannot access Metadata Manager data lineage from the PowerCenter Designer.**

In a split domain, the PowerCenter services in the primary domain do not communicate with the Metadata Manager Service in the secondary domain. Therefore, you cannot access Metadata Manager data lineage from the PowerCenter Designer.

## Model Repository Service

The Model Repository Service manages the Model repository. It receives requests from Informatica clients and application services to store or access metadata in the Model repository.

The following table summarizes the dependencies for products, services, and databases that are associated with the Model Repository Service.

Dependency	Summary
Products	The following products use the Model Repository Service: <ul style="list-style-type: none"><li>- Data Engineering Integration</li><li>- Data Engineering Quality</li><li>- Data Engineering Streaming</li><li>- Data Privacy Management</li><li>- Enterprise Data Catalog</li><li>- Enterprise Data Preparation</li><li>- Informatica Data Quality</li><li>- PowerCenter</li><li>- Test Data Management</li></ul>
Services	The Model Repository Service does not require an association with another application service.
Databases	The Model Repository Service uses the following database: <ul style="list-style-type: none"><li>- Model repository. Stores metadata created by Informatica clients and application services.</li></ul>
Installer	You can create the Model Repository Service when you run the installer.

## Model Repository Database Requirements

Informatica services and clients store data and metadata in the Model repository. Configure a monitoring Model repository to store statistics for ad hoc jobs, applications, logical data objects, SQL data services, web services, and workflows. Before you create the Model Repository Service, set up a database and database

user account for the Model repository. It is recommended that you use different database configuration for Model repository and monitoring Model repository.

The Model repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

When you configure Microsoft SQL Server, you can choose to configure the Microsoft Azure SQL Database as the Model repository.

If you specify the Windows NT credentials for the Model repository database on Microsoft SQL Server, you must also specify the connection string syntax to include the authentication method as NTLM.

Allow 3 GB of disk space for DB2. Allow 200 MB of disk space for all other database types.

For more information about configuring the database, see the documentation for your database system.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Specify the tablespace name when you use IBM DB2 as the Model Repository database.
- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2\_SKIPINSERTED
  - DB2\_EVALUNCOMMITTED
  - DB2\_SKIPDELETED
  - AUTO\_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a non-partitioned tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

## Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

**Note:** The guidelines to set up the repository for Azure SQL Database with Active Directory authentication is the same.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Specify the database schema name when you use Microsoft SQL Server as the Model Repository database.
- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

**Note:** The guidelines to set up the repositories for Microsoft Azure SQL Database and Azure SQL Database with Active Directory authentication is the same.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the OPEN\_CURSORS parameter to 4000 or higher.  
Verify that the database user has the following privileges:  
  
CREATE SEQUENCE  
  
CREATE SESSION  
  
CREATE SYNONYM  
  
CREATE TABLE  
  
CREATE VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- You can configure the connection between the Informatica domain, Model Repository Service, or PowerCenter Repository Service and Oracle RAC. Oracle Real Application Clusters (RAC) enables high availability of database applications. The Informatica domain, Model Repository Service, and PowerCenter Repository Service are resilient to failover of Oracle RAC databases for all CRUD operations. You cannot perform any administrator operations with Oracle RAC database failover for Informatica domain and Model Repository Service.

## PostgreSQL Database Requirements

Use the following guidelines when you set up the repository on PostgreSQL:

- Verify that the database user account has CONNECT, CREATE TABLE, and CREATE VIEW privileges.
- Specify the database schema name when you use PostgreSQL as the database.
- Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

<PostgreSQL installation directory>/data

- On the database, set the configuration parameters.

The following table lists the minimum and recommended values for the configuration parameters that you must set:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

# Monitoring Model Repository Service

The monitoring Model Repository Service is a Model Repository Service that monitors statistics for Data Integration Service jobs. You configure the monitoring Model Repository Service in the domain properties.

**Note:** If you want to generate monitoring statistics, you must create a dedicated Model Repository Service for monitoring. You cannot store run-time monitoring statistics in the same repository where you store object metadata.

The following table summarizes the dependencies for products, services, and databases that are associated with the monitoring Model Repository Service:

Dependency	Summary
Products	The following products use the monitoring Model Repository Service: <ul style="list-style-type: none"><li>- Data Engineering Integration</li><li>- Data Engineering Quality</li><li>- Data Engineering Streaming</li><li>- Data Privacy Management</li><li>- Enterprise Data Catalog</li><li>- Enterprise Data Preparation</li><li>- Informatica Data Quality</li><li>- PowerCenter</li><li>- Test Data Management</li></ul>
Services	The monitoring Model Repository Service does not require an association with another application service.
Databases	The monitoring Model Repository Service uses the following database: <ul style="list-style-type: none"><li>- Model repository. Stores run-time monitoring statistics that you can view in the Administrator tool.</li></ul>
Installer	You can create the monitoring Model Repository Service when you run the installer.

# PowerCenter Integration Service

The PowerCenter Integration Service receives requests from PowerCenter client tools to run data integration jobs. It writes results to different databases, and it writes run-time metadata to the PowerCenter repository. When you create the service, you need to associate another application service with it.

The following table lists the dependencies for products, services, and databases that are associated with the PowerCenter Integration Service.

Dependency	Summary
Products	The following products use the PowerCenter Integration Service: <ul style="list-style-type: none"><li>- PowerCenter</li><li>- Informatica Data Quality</li><li>- Test Data Management</li></ul>
Services	The PowerCenter Integration Service requires a direct association with the following service: <ul style="list-style-type: none"><li>- PowerCenter Repository Service</li></ul>

Dependency	Summary
Databases	The PowerCenter Integration Service does not have any associated database.
Installer	You can create the PowerCenter Integration Service when you run the installer.

## PowerCenter Repository Service

The PowerCenter Repository Service manages the PowerCenter repository. It receives requests from Informatica clients and application services to store or access metadata in the PowerCenter repository.

The following table summarizes the dependencies for products, services, and databases that are associated with the PowerCenter Repository Service.

Dependency	Summary
Products	The following products use the PowerCenter Repository Service: <ul style="list-style-type: none"> <li>- PowerCenter</li> <li>- Informatica Data Quality</li> <li>- Test Data Management</li> </ul>
Services	The PowerCenter Repository Service does not require an association with another application service.
Databases	The PowerCenter Repository Service uses the following database: <ul style="list-style-type: none"> <li>- PowerCenter repository. Stores metadata created by Informatica clients and application services.</li> </ul>
Installer	You can create the PowerCenter Repository Service when you run the installer.

## PowerCenter Repository Database Requirements

A PowerCenter repository is a collection of database tables containing metadata. A PowerCenter Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

The PowerCenter repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

**Note:** To create the PowerCenter Repository Service with the 10.5.3 installer, you can use the Oracle, Microsoft SQL Server, or the PostgreSQL database. If you want to install the PowerCenter Repository Service on any of the other databases, you create the service with the required database after you run the installer.

Allow 35 MB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the PowerCenter Repository Service.

For more information about configuring the database, see the documentation for your database system.



## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- To optimize repository performance, set up the database with the tablespace on a single node. When the tablespace is on one node, PowerCenter Client and PowerCenter Integration Service access the repository faster than if the repository tables exist on different database nodes.

Specify the single-node tablespace name when you create, copy, or restore a repository. If you do not specify the tablespace name, DB2 uses the default tablespace.

- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Verify that the database user account has the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.

The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY:

```
ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS
UNLIMITED PCTINCREASE 50 );
```

Verify or change the storage parameter for a tablespace before you create the repository.

- Verify that the database user has the following privileges:

```
CREATE SEQUENCE
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE VIEW
```

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- You can configure the connection between the Informatica domain, Model Repository Service, or PowerCenter Repository Service and Oracle RAC. Oracle Real Application Clusters (RAC) enables high availability of database applications. The Informatica domain, Model Repository Service, and PowerCenter Repository Service are resilient to failover of Oracle RAC databases for all CRUD operations. The following operations in the PowerCenter Repository Service are resilient to the database failover in Oracle RAC setup:

- ExecuteQuery
- ObjectExport

- ObjectImport
- PurgeVersion
- RollbackDeployment

## PostgreSQL Database Requirements

Use the following guidelines when you set up the repository on PostgreSQL:

### Privileges

Verify that the database user account has CREATE TABLE and CREATE VIEW privileges.

### Disk Space

Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

```
<PostgreSQL installation directory>/data
```

### Configuration Parameters

On the database, set the configuration parameters.

The following table lists the minimum and recommended values for the configuration parameters that you must set:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	4000
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

### Configuring PostgreSQL for the PowerCenter repository

To configure a PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the pg\_service.conf file in the following format:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter repository database service name
```

Ensure that the entries for the [PCRS\_DB\_SERVICE\_NAME] entry match the configuration for the PowerCenter Repository Service. To securely connect to PostgreSQL for the PowerCenter repository, set the security property along with the remaining required database properties in the pg\_service.conf file in the following format: `sslmode=require` Set the PGSERVICEFILE environment variable to the location of the pg\_service.conf file. The pg\_service.conf file contains the connection parameters for PostgreSQL database connection in the Informatica installation directory. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Using a C shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file  
directory>/pg_service.conf
```

## Sybase ASE Database Requirements

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.
- Set the database memory configuration requirements.

The following table lists the memory configuration requirements and the recommended baseline values:

Database Configuration	Sybase System Procedure	Value
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	8000
Number of locks	sp_configure "number of locks"	100000

## Search Service

The Search Service manages searches in the Analyst tool and returns search results from the Model repository. When you create the service, you need to associate another application service with it.

The following table summarizes the dependencies for products, services, and databases that are associated with the Search Service:

Dependency	Summary
Products	The following products use the Search Service: <ul style="list-style-type: none"><li>- Data Engineering Integration</li><li>- Data Engineering Quality</li><li>- Data Engineering Streaming</li><li>- Enterprise Data Catalog</li><li>- Enterprise Data Preparation</li><li>- Informatica Data Quality</li><li>- PowerCenter</li></ul>
Services	The Search Service requires a direct association with the following service: <ul style="list-style-type: none"><li>- Model Repository Service</li></ul>

Dependency	Summary
Databases	The Search Service is not associated with any database.
Installer	You cannot create the Search Service when you run the installer.

## Configure Native Connectivity on Service Machines

To establish native connectivity between an application service and a database, install the database client software for the database that you want to access.

Native drivers are packaged with the database server and client software. Configure connectivity on the machines that need to access the databases. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries.

The following services use native connectivity to connect to different databases:

### Data Integration Service

The Data Integration Service uses native database drivers to connect to the following databases:

- Source and target databases. Reads data from source databases and writes data to target databases.
- Data object cache database. Stores the data object cache.
- Profiling source databases. Reads from relational source databases to run profiles against the sources.
- Profiling warehouse. Writes the profiling results to the profiling warehouse.
- Reference tables. Runs mappings to transfer data between the reference tables and the external data sources.

When the Data Integration Service runs on a single node or on primary and back-up nodes, install database client software and configure connectivity on the machines where the Data Integration Service runs.

When the Data Integration Service runs on a grid, install database client software and configure connectivity on each machine that represents a node with the compute role or a node with both the service and compute roles.

### PowerCenter Repository Service

The PowerCenter Repository Service uses native database drivers to connect to the PowerCenter repository database.

Install database client software and configure connectivity on the machines where the PowerCenter Repository Service and the PowerCenter Repository Service processes run.

### PowerCenter Integration Service

The PowerCenter Integration Service uses native database drivers to connect to the following databases:

- Source and target databases. Reads from the source databases and writes to the target databases.
- Metadata Manager source databases. Loads the relational data sources in Metadata Manager.

Install database client software associated with the relational data sources and the repository databases on the machines where the PowerCenter Integration Service runs.

## Install Database Client Software

You must install the database clients on the required machines based on the types of databases that the application services access.

To ensure compatibility between the application service and the database, use the appropriate database client libraries and install a client software that is compatible with the database version.

Install the following database client software based on the type of database that the application service accesses:

### **IBM DB2 Client Application Enabler (CAE)**

Configure connectivity on the required machines by logging in to the machine as the user who starts Informatica services.

### **Microsoft SQL Server 2014 Native Client**

Download the client from the following Microsoft website:  
<http://www.microsoft.com/en-in/download/details.aspx?id=42295>.

### **Oracle client**

Install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

### **Sybase Open Client (OCS)**

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

### **PostgreSQL client (psql)**

Install and run the PostgreSQL interactive terminal program called psql, which allows you to interactively enter, edit, and run SQL commands.

psql is a terminal-based front-end to PostgreSQL. You can type in queries interactively, issue the queries to PostgreSQL, and check the query results. Or, the input can be from a file or from command line arguments.

You can install psql client application for PostgreSQL to work only on Linux or Windows.

Install and run the required software dependency packages to build PostgreSQL, such as GCC compiler package, readline and readline-devel packages, and zlib-devel compression library package. After you install the packages from the GNU Readline library, psql remembers each command you type, and you can use arrow keys to recall and edit previous commands.

You can also run the required library files with the yum install commands.

### **PostgreSQL on Windows**

On Windows, download the psql client from the following link:

<https://www.enterprisedb.com/downloads/postgres-postgresql-downloads>

You must verify that PostgreSQL libraries are present in the following directories on Windows:

- Installation directory: C:\Program Files\PostgreSQL\10
- Command line tools installation directory: C:\Program Files\PostgreSQL\10

- pgAdmin4 installation directory: C:\Program Files\PostgreSQL\10\pgAdmin 4

#### PostgreSQL on Linux

On Linux, you also need to install the required PostgreSQL libraries,  
 postgresql10-10.10-1PGDG.rhel7.x86\_64 and postgresql10-libs-10.10-1PGDG.rhel7.x86\_64

For more information about psql, see the psql client documentation in the following link:  
<https://www.postgresql.org/docs/10/app-psql.html>

## Configure Database Client Environment Variables

Configure database client environment variables on the machines that run the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes.

After you configure the database environment variables, you can test the connection to the database from the database client.

### Oracle database

The following table lists the database environment variables that you need to set for the Oracle database with `sqlplus` as the database utility:

Environment Variable	Value
ORACLE_HOME	<Client InstallDatabasePath>
PATH	<DatabasePath>/bin and USER_INSTALL_DIR/server/bin:\$PATH
LD_LIBRARY_PATH	\$Oracle_HOME/lib and USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH
TNS_ADMIN	Set to the location of the tnsnames.ora file: \$ORACLE_HOME/network/admin
INFA_TRUSTSTORE	For default SSL domain, add to: USER_INSTALL_DIR/services/shared/security For custom SSL domain, set INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD

### IBM DB2 database

The following table lists the database environment variables that you need to set for the IBM DB2 database with `db2connect` as the database utility:

Environment Variable	Value
DB2DIR	<database path>
DB2INSTANCE	<DB2InstanceName>
PATH	<database path>/bin

## Sybase ASE database

The following table lists the database environment variables that you need to set for the Sybase ASE database with `isql` as the database utility:

Environment Variable	Value
SYBASE15	<<database path>/sybase<version> >
SYBASE_ASE	\${SYBASE15}/ASE-<version>
SYBASE_OCS	\${SYBASE15}/OCS-<version>
PATH	\${SYBASE_ASE}/bin:\${SYBASE_OCS}/bin:\$PATH

## PostgreSQL database

The following table lists the database environment variables that you need to set for the PostgreSQL database:

Environment Variable	Value
PGSERVICEFILE	Set to the location of the <code>pg_service.conf</code> file: <pg_service.conf file directory>/ <code>pg_service.conf</code>
PGHOME	<code>/usr/pgsql-10</code>
PATH	<code>\$PGHOME:\${PATH}</code>
LD_LIBRARY_PATH	<code>\$PGHOME/lib:\${LD_LIBRARY_PATH}</code>
INFA_TRUSTSTORE	For default SSL domain, add to: <InstallationDirectory>/services/shared/security For custom SSL domain, set <code>INFA_TRUSTSTORE</code> and <code>INFA_TRUSTSTORE_PASSWORD</code>
POSTGRES_ODBC	Set the value to 1 for the PostgreSQL ODBC connection. You can set it for all the repositories in the domain or for any PostgreSQL repository that uses an ODBC connection.

## Microsoft SQL Server database

The following table lists the database environment variables that you need to set for the Microsoft SQL Server database:

Environment Variable	Value
ODBCHOME	<code>USER_INSTALL_DIR/ODBC7.1</code>
ODBCINI	<code>\$ODBCHOME/odbc.ini</code>
ODBCINST	<code>\$ODBCHOME/odbcinst.ini</code>
PATH	<code>/opt/mssql-tools/bin:\$PATH\$PATHUSER_INSTALL_DIR/ODBC7.1:\$PATHUSER_INSTALL_DIR/server/bin:\$PATH</code>

Environment Variable	Value
LD_LIBRARY_PATH	<i>\$ODBCHOME/lib</i>
INFA_TRUSTSTORE	<i>USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH</i> For default SSL domain, add to: <i>USER_INSTALL_DIR/services/shared/security</i> For custom SSL domain, set INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD



## CHAPTER 5

# Prepare for Kerberos Authentication

This chapter includes the following topics:

- [Checklist to Prepare for Kerberos Authentication , 81](#)
- [Prepare for Kerberos Authentication Overview, 81](#)
- [Set Up the Kerberos Configuration File, 82](#)
- [Generate the Service Principal and Keytab File Name Format, 83](#)
- [Review the SPN and Keytab Format Text File, 86](#)
- [Create the Service Principal Names and Keytab Files, 88](#)

## Checklist to Prepare for Kerberos Authentication

This chapter contains tasks to perform if you want the installer to enable Kerberos during installation. Use this checklist to track tasks required to prepare for Kerberos authentication.

- ☐ Set up the Kerberos configuration file.
- ☐ Generate the service principal and keytab name file format.
- ☐ Review the SPN and keytab format text file.
- ☐ Create the SPN and keytab files.

## Prepare for Kerberos Authentication Overview

You can configure the Informatica domain to use Kerberos network authentication to authenticate users, services, and nodes.

Kerberos is a network authentication protocol which uses tickets to authenticate access to services and nodes in a network. Kerberos uses a Key Distribution Center (KDC) to validate the identities of users and services and to grant tickets to authenticated user and service accounts. In the Kerberos protocol, users and services are known as principals. The KDC has a database of principals and their associated secret keys that are used as proof of identity. Kerberos can use an LDAP directory service as a principal database.

To use Kerberos authentication, you must install and run the Informatica domain on a network that uses Kerberos network authentication. Informatica can run on a network that uses Kerberos authentication with Microsoft Active Directory service as the principal database.

The Informatica domain requires keytab files to authenticate nodes and services in the domain without transmitting passwords over the network. The keytab files contain the service principal names (SPN) and associated encrypted keys. Create the keytab files before you create nodes and services in the Informatica domain.

**Note:** Enterprise Data Catalog or Enterprise Data Preparation does not support an Informatica domain enabled for Kerberos authentication.

## Set Up the Kerberos Configuration File

Kerberos stores configuration information in a file named *krb5.conf*. Informatica requires specific properties set in the Kerberos configuration file so that the Informatica domain can use Kerberos authentication correctly. You must set the properties in the *krb5.conf* configuration file.

The configuration file contains the information about the Kerberos server, including the Kerberos realm and the address of the KDC. You can request the Kerberos administrator to set the properties in the configuration file and send you a copy of the file.

1. Back up the *krb5.conf* file before you make any changes.
2. Edit the *krb5.conf* file.
3. In the *libdefaults* section, set or add the properties required by Informatica.

The following table lists the values to which you must set properties in the *libdefaults* section:

Parameter	Value
default_realm	Name of the service realm for the Informatica domain. If you are integrating the domain with a non-native environment, set the <i>default_realm</i> property to be the same as the <i>default_realm</i> property of the cluster.
forwardable	Allows a service to delegate client user credentials to another service. Set this parameter to True. The Informatica domain requires application services to authenticate the client user credentials with other services.
default_tkt_enctypes	Encryption types for the session key in ticket-granting tickets (TGT). Set this parameter only if session keys must use specific encryption types.
udp_preference_limit	Determines the protocol that Kerberos uses when it sends a message to the KDC. Set <i>udp_preference_limit</i> = 1 to always use TCP. The Informatica domain supports only the TCP protocol. If the <i>udp_preference_limit</i> is set to any other value, the Informatica domain might shut down unexpectedly.

4. In the *realms* section, include the port number in the address of the KDC separated by a colon.  
For example, if the KDC address is *kerberos.example.com* and the port number is 88, set the *kdc* parameter to the following:

```
kdc = kerberos.example.com:88
```

5. Save the *krb5.conf* file.

6. Store the `krb5.conf` file in a directory that is accessible to the machine where you plan to install the Informatica services.

The following example shows the content of a `krb5.conf` with the required properties:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
    admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
    kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
}

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

For more information about the Kerberos configuration file, see the Kerberos network authentication documentation.

## Generate the Service Principal and Keytab File Name Format

If you run the Informatica domain with Kerberos authentication, you must associate Kerberos service principal names (SPN) and keytab files with the nodes and processes in the Informatica domain. Informatica requires keytab files to authenticate services without requests for passwords.

Based on the security requirements for the domain, you can set the service principal level to one of the following levels:

### Node Level

If the domain is used for testing or development and does not require a high level of security, you can set the service principal at the node level. You can use one SPN and keytab file for the node and all the service processes on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

### Process Level

If the domain is used for production and requires a high level of security, you can set the service principal at the process level. Create a unique SPN and keytab file for each node and each process on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

The Informatica domain requires the service principal and keytab file names to follow a specific format. To ensure that you follow the correct format for the service principal and keytab file names, use the Informatica Kerberos SPN Format Generator to generate a list of the service principal and keytab file names in the format required by the Informatica domain.

The Informatica Kerberos SPN Format Generator is shipped with the Informatica services installer.

## Service Principal Requirements at Node Level

If the Informatica domain does not require a high level of security, the node and service processes can share the same SPNs and keytab files. The domain does not require a separate SPN for each service process in a node.

The Informatica domain requires SPNs and keytab files for the following components at node level:

### **Principal distinguished name (DN) for the LDAP directory service**

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

### **Node process**

Principal name for the Informatica node that initiates or accepts authentication calls. The same principal name is used to authenticate the services in the node. Each gateway node in the domain requires a separate principal name.

### **HTTP processes in the domain**

Principal name for all web application services in the Informatica domain, including Informatica Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

## Service Principal Requirements at Process Level

If the Informatica domain requires a high level of security, create a separate SPN and keytab file for each node and each service in the node.

The Informatica domain requires SPNs and keytab files for the following components at process level:

### **Principal distinguished name (DN) for the LDAP directory service**

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

### **Node process**

Principal name for the Informatica node that initiates or accepts authentication calls.

### **Informatica Administrator service**

Principal name for the Informatica Administrator service that authenticates the service with other services in the Informatica domain. The name of the keytab file must be `be_AdminConsole.keytab`.

### **HTTP processes in the domain**

Principal name for all web application services in the Informatica domain, including Informatica Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

### **Service process**

Principal name for the service that runs on a node in the Informatica domain. Each service requires a unique service principal and keytab file name.

You do not need to create the SPNs and keytab files for the services before you run the installer. You can create the SPN and keytab file for a service when you create the service in the domain. The SPN and keytab file for a service must be available when you enable the service.

## Running the SPN Format Generator

You can run the Informatica Kerberos SPN Format Generator to generate a file that shows the correct format for the SPNs and keytab file names required in the Informatica domain.

You can run the SPN Format Generator from the command line or from the Informatica installer. The SPN Format Generator generates a file with the names of the service principal and keytab files based on the parameters you provide.

**Note:** Verify that the information you provide is correct. The SPN Format Generator does not validate the values you enter.

1. On the machine where you extracted the installation files, go to the following directory: `<Informatica installation files directory>/Server/Kerberos`
2. On a shell command line, run the SPNFormatGenerator file.
3. Press **Enter** to continue.
4. In the **Service Principal Level** section, select the level at which to set the Kerberos service principals for the domain.

The following table describes the levels you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node.  The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node.  This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node.  Use the node level option for domains that do not require a high level of security, such as test and development domains.

5. Enter the domain and node parameters required to generate the SPN format.

The following table describes the parameters you must specify:

Prompt	Description
Domain Name	Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the Informatica node.

Prompt	Description
Node host name	Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character. <b>Note:</b> Do not use <i>localhost</i> . The host name must explicitly identify the machine.
Service Realm Name	Name of the Kerberos realm for the Informatica domain services. The realm name must be in uppercase.

If you set the service principal at node level, the prompt **Add Node?** appears. If you set the service principal at process level, the prompt **Add Service?** appears.

- At the **Add Node?** prompt, enter 1 to generate the SPN format for an additional node. Then enter the node name and node host name.  
To generate the SPN formats for multiple nodes, enter 1 at each **Add Node?** prompt and enter a node name and node host name.
- At the **Add Service?** prompt, enter 1 to generate the SPN format for a service that will run on the preceding node. Then enter the service name.  
To generate the SPN formats for multiple services, enter 1 at each **Add Service?** prompt and enter a service name.
- Enter 2 to end the **Add Service?** or **Add Node?** prompts.  
The SPN Format Generator displays the path and file name of the file that contains the list of service principal and keytab file names.
- Press Enter to exit the SPN Format Generator.  
The SPN Format Generator generates a text file that contains the SPN and keytab file names in the format required for the Informatica domain.

## Review the SPN and Keytab Format Text File

The Kerberos SPN Format Generator generates a text file named SPNKeytabFormat.txt that lists the format for the service principal and keytab file names required by the Informatica domain. The list includes the SPN and keytab file names based on the service principal level you select.

Review the text file and verify that there are no error messages.

The text file contains the following information:

### Entity Name

Identifies the node or service associated with the process.

### SPN

Format for the SPN in the Kerberos principal database. The SPN is case sensitive. Each type of SPN has a different format.

An SPN can have one of the following formats:

Keytab type	SPN Format
NODE_SPN	isp/<NodeName>/<DomainName>@<REALMNAME>
NODE_AC_SPN	_AdminConsole/<NodeName>/<DomainName>@<REALMNAME>
NODE_HTTP_SPN	HTTP/<NodeHostName>@<REALMNAME> <b>Note:</b> The Kerberos SPN Format Generator validates the node host name. If the node host name is not valid, the utility does not generate an SPN. Instead, it displays the following message: Unable to resolve host name.
SERVICE_PROCESS_SPN	<ServiceName>/<NodeName>/<DomainName>@<REALMNAME>

### Keytab File Name

Format for the name of the keytab file to be created for the associated SPN in the Kerberos principal database. The keytab file name is case sensitive.

The keytab file names use the following formats:

Keytab type	Keytab File Name
NODE_SPN	<NodeName>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<ServiceName>.keytab

### Keytab Type

Type of the keytab. The keytab type can be one of the following types:

- NODE\_SPN. Keytab file for a node process.
- NODE\_AC\_SPN. Keytab file for the Informatica Administrator service process.
- NODE\_HTTP\_SPN. Keytab file for HTTP processes in a node.
- SERVICE\_PROCESS\_SPN. Keytab file for a service process.

### Service Principals at Node Level

The following example shows the contents of the SPNKeytabFormat.txt file generated for service principals at the node level:

ENTITY_NAME	SPN	KEY_TAB_NAME
KEY_TAB_TYPE		
Node01	isp/Node01/Infadomain@MY.SVCREALM.COM	Node01.keytab
NODE_SPN		
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node02	isp/Node02/Infadomain@MY.SVCREALM.COM	Node02.keytab
NODE_SPN		
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node03	isp/Node03/Infadomain@MY.SVCREALM.COM	Node03.keytab
NODE_SPN		

```
Node03          HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM    webapp_http.keytab
NODE_HTTP_SPN
```

## Service Principals at Process Level

The following example shows the contents of the SPNKeytabFormat.txt file generated for service principals at the process level:

```
ENTITY_NAME      SPN
KEY_TAB_NAME     KEY_TAB_TYPE
Node01           isp/Node01/Infadomain@MY.SVCREALM.COM
Node01.keytab    NODE_SPN
Node01           AdminConsole/Node01/Infadomain@MY.SVCREALM.COM
_AdminConsole.keytab NODE_AC_SPN
Node01           HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab NODE_HTTP_SPN
Node02           isp/Node02/Infadomain@MY.SVCREALM.COM
Node02.keytab    NODE_SPN
Node02           AdminConsole/Node02/Infadomain@MY.SVCREALM.COM
_AdminConsole.keytab NODE_AC_SPN
Node02           HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab NODE_HTTP_SPN
Service10:Node01 Service10/Node01/Infadomain@MY.SVCREALM.COM
Service10.keytab SERVICE_PROCESS_SPN
Service100:Node02 Service100/Node02/Infadomain@MY.SVCREALM.COM
Service100.keytab SERVICE_PROCESS_SPN
Service200:Node02 Service200/Node02/Infadomain@MY.SVCREALM.COM
Service200.keytab SERVICE_PROCESS_SPN
```

# Create the Service Principal Names and Keytab Files

After you generate the list of SPN and keytab file names in Informatica format, send a request to the Kerberos administrator to add the SPNs to the Kerberos principal database and create the keytab files.

Use the following guidelines when you create the SPN and keytab files:

**The user principal name (UPN) must be the same as the SPN.**

When you create a user account for the service principal, you must set the UPN with the same name as the SPN. The application services in the Informatica domain can act as a service or a client depending on the operation. You must configure the service principal to be identifiable by the same UPN and SPN.

A user account must be associated with only one SPN. Do not set multiple SPNs for one user account.

**Enable delegation in Microsoft Active Directory.**

You must enable delegation for all user accounts with service principals used in the Informatica domain. In the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

Delegated authentication happens when a user is authenticated with one service and that service uses the credentials of the authenticated user to connect to another service. Because services in the Informatica domain need to connect to other services to complete an operation, the Informatica domain requires the delegation option to be enabled in Microsoft Active Directory.

**Use the ktpass utility to create the service principal keytab files.**

Microsoft Active Directory supplies the ktpass utility to create keytab files. Informatica supports Kerberos authentication only on Microsoft Active Directory and has certified only keytab files that are created with ktpass.



The keytab files for a node must be available on the machine that hosts the node. By default, the keytab files are stored in the following directory: <Informatica installation directory>/isp/config/keys. During installation, you can specify a directory on the node to store the keytab files.

When you receive the keytab files from the Kerberos administrator, copy the keytab files to a directory that is accessible to the machine where you plan to install the Informatica services. When you run the Informatica installer, specify the location of the keytab files. The Informatica installer copies the keytab files to the directory for keytab files on the Informatica node.

## Troubleshooting the Service Principal Names and Keytab Files

You can use Kerberos utilities to verify that the service principal and keytab file names created by the Kerberos administrator match the service principal and keytab file names that you requested. You can also use the utilities to determine the status of the Kerberos key distribution center (KDC).

You can use Kerberos utilities such as *setspn*, *kinit* and *klist* to view and verify the SPNs and keytab files. To use the utilities, ensure that the KRB5\_CONFIG environment variable contains the path and file name of the Kerberos configuration file.

**Note:** The following examples show ways to use the Kerberos utilities to verify that SPNs and keytab files are valid. The examples might be different than the way that the Kerberos administrator uses the utilities to create the SPNs and keytab files required for the Informatica domain. For more information about running the Kerberos utilities, see the Kerberos documentation.

Use the following utilities to verify the SPNs and keytab files:

### klist

You can use *klist* to list the Kerberos principals and keys in a keytab file. To list the keys in the keytab file and the time stamp for the keytab entry, run the following command:

```
klist -k -t <keytab_file>
```

The following output example shows the principals in a keytab file:

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp Principal
-----
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

### kinit

You can use *kinit* to request a ticket-granting ticket for a user account to verify that the KDC is running and can grant tickets. To request a ticket-granting ticket for a user account, run the following command:

```
kinit <user_account>
```

You can also use *kinit* to request a ticket-granting ticket and verify that the keytab file can be used to establish a Kerberos connection. To request a ticket-granting ticket for an SPN, run the following command:

```
kinit -V -k -t <keytab_file> <SPN>
```

The following output example shows the ticket-granting ticket created in the default cache for a specified keytab file and SPN:

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

## setspn

You can use *setspn* to view, modify, or delete the SPN of an Active Directory service account. On the machine that hosts the Active Directory service, open a command line window and run the command.

To view the SPNs that are associated with a user account, run the following command:

```
setspn -L <user_account>
```

The following output example shows the SPN associated with the user account *is96svc*:

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,  
DC=ds,DC=intrac0rp,DC=zec0rp:  
    int_srvc01/node02_vMPE/Domn96_vMPE
```

To view the user accounts associated with an SPN, run the following command:

```
setspn -Q <SPN>
```

The following output example shows the user account associated with the SPN *int\_srvc01/node02\_vMPE/Domn96\_vMPE*:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp  
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp  
    int_srvc01/node02_vMPE/Domn96_vMPE
```

```
Existing SPN found!
```

To search for duplicate SPNs, run the following command:

```
setspn -X
```

The following output example shows multiple user accounts associated with one SPN:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp  
Processing entry 1125  
HOST/mtb01.REALM is registered on these accounts:  
    CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp  
    CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

**Note:** Searching for duplicate SPNs can take a long time and a large amount of memory.

## kdestroy

You can use *kdestroy* to delete the active Kerberos authorization tickets and the user credentials cache that contains them. If you run *kdestroy* without parameters, you delete the default credentials cache.

## CHAPTER 6

# Record Information for Installer Prompts

This chapter includes the following topics:

- [Checklist to Record Installer Prompts, 91](#)
- [Record Information for Installer Prompts Overview, 92](#)
- [Domain, 92](#)
- [Nodes, 93](#)
- [Distribution Packages, 93](#)
- [Application Services, 93](#)
- [Databases , 94](#)
- [Connection String to a Secure Database, 96](#)
- [Secure Data Storage, 98](#)
- [Kerberos, 98](#)

## Checklist to Record Installer Prompts

This chapter contains information that you need to enter when you run the installer. Use this checklist to track the recording tasks before you run the installer.

- ☐ Record the names of nodes that you want to create and the services that you want to create on each node.
- ☐ Record basic database information for each database associated with a service that you are creating.
- ☐ If the domain configuration and Model repository databases are secure, record the JDBC connection string with required security parameters.
- ☐ Record the site key for the installer.
- ☐ If you want to enable Kerberos authentication when you run the installer, record Kerberos information for each node in the domain.

# Record Information for Installer Prompts Overview

When you install the Informatica services, you need to know information about the domain, nodes, application services, databases, and distribution packages for the environment.

This section lists information that you need to provide when you run the installer. Informatica recommends recording installer prompts before you start the installation process. For example, you might want to create a text file of information so you can copy into the installer.

## Domain Object Naming Conventions

You cannot change domain, node, and application service names. Use names that continue to work if you migrate a node to another machine or if you add additional nodes and services to the domain. In addition, use names that convey how the domain object is used. Naming conventions are provided in applicable topics.

## Domain

When you create a domain, you must provide a domain name and gateway node name.

The following table describes the domain information that you need to enter during the installation process:

Domain Information	Description
Domain name	Name of the domain that you plan to create. The name must not exceed 128 characters and must be 7-bit ASCII only. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ / Consider one of the following naming conventions: DMN, DOM, DOMAIN, _<ORG>_<ENV>
Master gateway node host name	Fully qualified host name of the machine on which to create the master gateway node. If the machine has a single network name, use the default host name. The node host name cannot contain the underscore (_) character. If the machine has multiple network names, you can modify the default host name to use an alternate network name. If the machine has a single network name, use the default host name. <b>Note:</b> Do not use localhost. The host name must explicitly identify the machine.
Master gateway node name	Name of the master gateway node that you plan to create on this machine. The node name is not the host name for the machine. Consider the following naming convention: Node<node##>_<ORG>_<optional distinguisher>_<ENV>

# Nodes

When you install the Informatica services, you add the installation machine to the domain as a node. You can add multiple nodes to a domain.

The following table describes the node information that you need to enter when you join a domain.

Node Information	Description
Node host name	Fully qualified host name of the machine on which to create nodes. If the machine has a single network name, use the default host name. The node host name cannot contain the underscore (_) character.  If the machine has multiple network names, you can modify the default host name to use an alternate network name. If the machine has a single network name, use the default host name. <b>Note:</b> Do not use localhost. The host name must explicitly identify the machine.
Node name	Name of the nodes that you plan to create on this machine. The node name is not the host name for the machine.  Consider the following naming convention: Node<node##>_<ORG>_<optional distinguisher>_<ENV>

## Distribution Packages

If you are going to install a distribution package through the installer, record the distribution package that you downloaded.

## Application Services

Record the application service names and the nodes where you want to create them.

The following table lists the application services that you can create when you run the installer:

Application Service	Naming Convention
Catalog Service	CS_<ORG>_<ENV>
Content Management	CMS_<ORG>_<ENV>
Data Integration Service	DIS_<ORG>_<ENV>
Data Privacy Management Service	DPM_<ORG>_<ENV>
Interactive Data Preparation Service	DPS_<ORG>_<ENV>
Enterprise Data Preparation Service	EDLS_<ORG>_<ENV>
Metadata Access Service	MAS_<ORG>_<ENV>

Application Service	Naming Convention
Informatica Cluster Service	ICS_<ORG>_<ENV>
Model Repository Service	MRS_<ORG>_<ENV>
monitoring Model Repository Service	mMRS_<ORG>_<ENV>
PowerCenter Repository Service	PCRS, RS _<ORG>_<ENV>
PowerCenter Integration Service	PCIS, IS _<ORG >_<ENV>

For more information about all service naming conventions, see the following Informatica Velocity Best Practice article available on the Informatica Network: [Velocity Naming Conventions](#)

**Important:** If you plan to use Kerberos authentication, you must know the application service and node name before you create the keytab files.

## Databases

When you plan the installation, you also need to plan the required relational databases. The domain requires a database to store configuration information and user account privileges and permissions. Some application services require databases to store information processed by the application service.

### Domain

The following table describes the information that you need to enter during the installation process:

Database Information	Description
Domain configuration database type	Database type for the domain configuration repository. The domain configuration repository supports IBM DB2 UDB, Microsoft SQL Server, Oracle, PostgreSQL, or Sybase ASE.
Domain configuration database host name	The name of the machine hosting the database.

### Content Management Service

The following table describes the information that you need to enter during the installation process:

Database Information	Description
Reference data warehouse database type	Database type for the reference data warehouse. The reference data warehouse supports IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle, or PostgreSQL.
Reference data warehouse database host name	The name of the machine hosting the database.

## Data Integration Service

The following table describes the information that you need to enter during the installation process:

Database Information	Description
Data object cache database type	Database type for the data object cache database. The data object cache database supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.
Data object cache database host name	The name of the machine hosting the database.
Profiling warehouse database type	Database type for the profiling warehouse. The profiling warehouse supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.
Profiling warehouse database host name	The name of the machine hosting the database.
Workflow database type	Database type for the workflow database. The workflow database supports IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle, or PostgreSQL.
Workflow database host name	The name of the machine hosting the database.

## Model Repository Service

The following table describes the information that you need to enter during the installation process:

Database Information	Description
Model repository database type	Database type for the Model repository. The Model repository supports IBM DB2 UDB, Microsoft SQL Server, PostgreSQL, or Oracle.
Model repository database host name	The name of the machine hosting the database.

## PowerCenter Repository Service

The following table describes the information that you need to enter during the installation process:

Database Information	Description
PowerCenter repository database type	Database type for the PowerCenter repository. The PowerCenter repository supports IBM DB2 UDB, Microsoft SQL Server, Oracle, or PostgreSQL.
PowerCenter repository database host name	The name of the machine hosting the database.

# Connection String to a Secure Database

If you create a repository on a secure database, you must provide the truststore information for the database and a JDBC connection string that includes the security parameters for the database.

During installation, you can create the domain configuration repository in a secure database. You can also create the Model repository and PowerCenter repository in a secure database.

You can configure a secure connection to the following databases:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- PostgreSQL
- Azure PostgreSQL
- Oracle

**Note:** You cannot configure a secure connection to a Sybase database.

When you configure the connection to the secure database, you must specify the connection information in a JDBC connection string. In addition to the host name and port number for the database server, the connection string must include security parameters.

The following table describes the security parameters that you must include in the JDBC connection string:

Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to <code>SSL</code> .
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that is sent by the database server.  If this parameter is set to <code>True</code> , Informatica validates the certificate that is sent by the database server. If you specify the <code>HostNameInCertificate</code> parameter, Informatica also validates the host name in the certificate.  If this parameter is set to <code>false</code> , Informatica doesn't validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.  If SSL encryption and validation is enabled and this property is not specified, the driver uses the server name specified in the connection URL or data source of the connection to validate the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to <code>cryptoProtocolVersion=TLSv1.1</code> or <code>cryptoProtocolVersion=TLSv1.2</code> based on the cryptographic protocol used by the database server.

You can use the following syntax in the JDBC connection string to connect to a secure database:



## IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

## Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;
```

## Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

### Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

## Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

## PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

## Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

**Note:** The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

# Secure Data Storage

When you install the Informatica services, you must back up the site key that the installer generates and ensure that you save the site key. If you lose the site key, you cannot generate the site key again.

Use the following table to record the information that you need to configure secure data storage:

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: <Informatica installation directory>/isp/config/keys.
Specify if you want to back up the site key that the installer generates or not:	<p>Specify if you want to back up the site key that the installer generates or not:</p> <ul style="list-style-type: none"><li>- Select <b>1</b> for No. If you choose No, the installer exits.</li><li>- Select <b>2</b> for Yes. If you choose Yes, you agree to back up the file manually.</li></ul> <p>A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.</p>

## Kerberos

When you install the Informatica application services, you can enable options in the Informatica domain to configure security for the domain, services and databases.

If you want to enable Kerberos authentication and you do not want to use the default file, you need to provide information such as keystore and truststore directories. Each node needs to contain a keystore and truststore that is used by all services on that node.

The following table describes security information to provide during installation:

Security Information	Description
Service realm name	<p>Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase.</p> <p>The service realm name and the user realm name must be the same.</p>
User realm name	<p>Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase.</p> <p>The service realm name and the user realm name must be the same.</p>
Location of the Kerberos configuration file	<p>Directory where the Kerberos configuration file named <i>krb5.conf</i> is stored. Informatica requires specific properties to be set in the configuration file. If you do not have permission to copy or update the Kerberos configuration file, you might have to request the Kerberos administrator to update the file.</p>
Keystore file directory	<p>Directory that contains the keystore files. The directory must contain files named <i>infa_keystore.jks</i> and <i>infa_keystore.pem</i>.</p>
Keystore password	<p>A plain-text password for the keystore <i>infa_keystore.jks</i>.</p>

Security Information	Description
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

## CHAPTER 7

# Introduction to the Services Installer

This chapter includes the following topics:

- [Services Installer Tasks, 100](#)
- [Secure Files and Directories, 100](#)
- [Pre-install Utilities, 101](#)
- [Run the Pre-Installation \(i10Pi\) System Check Tool in Console Mode, 101](#)
- [Run the Pre-Installation \(i10Pi\) System Check Tool in Graphical Mode, 105](#)
- [Run the Pre-Installation \(i10Pi\) System Check Tool in Silent Mode, 110](#)

## Services Installer Tasks

The installer performs install tasks based on the product or products that you install.

The installer can perform the following tasks:

1. Perform pre-install validation and system check.
2. Create a domain or join a node to an existing domain.
3. Install binaries for service support.
4. Create application services.
5. Configure security between the domain and services.
6. Start the domain and application services that you created.
7. Write message to the log file.

## Secure Files and Directories

When you install or upgrade Informatica, the installer creates directories to store Informatica files that require restricted access, such as the domain encryption key file and the nodemeta.xml. The installer assigns different permissions for the directories and the files in the directories.

By default, the installer creates the following directories within the Informatica installation directory:

#### **<Informatica installation directory>/isp/config**

Contains the nodemeta.xml file. Also contains the /keys directory where the encryption key file is stored. If you configure the domain to use Kerberos authentication, the /keys directory also contains the Kerberos keytab files. You can specify a different directory in which to store the files. The installer assigns the same permissions to the specified directory as the default directory.

#### **<Informatica installation directory>/services/shared/security**

If you enable secure communication for the domain, the /security directory contains the keystore and truststore files for the default SSL certificates.

To maintain the security of the directories and files, the installer restricts access to the directories and the files in the directories. The installer assigns specific permissions to the group and user account that own the directories and files.

For more information about permissions assigned to the directories and files, see the Informatica Security Guide.

## Pre-install Utilities

Informatica provides utilities to facilitate the Informatica services installation process. You can use the Informatica installer to run the utilities.

Run the following utilities before you install Informatica services:

#### **Pre-Installation (i10Pi) System Check Tool**

The Pre-Installation (i10Pi) System Check Tool verifies whether a machine meets the system requirements for the Informatica installation. Informatica recommends that you verify the minimum system requirements before you start the installation. When you run the system check tool before you perform the installation, the installer sets fields for certain fields, such as the database connection and domain port numbers, based on the information that you enter during the system check.

#### **Informatica Kerberos SPN Format Generator**

The Informatica Kerberos SPN Format Generator generates a list of Kerberos service principal names (SPN) and keytab file names in the format required by Informatica. If you install Informatica on a network that uses Kerberos authentication, run this utility to generate the service principal and keytab file names in the informatica format. Then request the Kerberos administrator to add the SPNs to the Kerberos principal database and create the keytab files before you start the installation.

## Run the Pre-Installation (i10Pi) System Check Tool in Console Mode

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation or upgrade.

Ensure that you verified the system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.

2. Close all other applications.
3. On a shell command line, run the install file.  
The installer displays the message to verify that the locale environment variables are set.
4. If the environment variables are not set, press **n** to exit the installer and set them as required.  
If the environment variables are set, press **y** to continue.
5. Press **1** to install or upgrade Informatica.
6. Press **1** to run the Pre-Installation (i10Pi) System Check Tool that verifies whether the machine meets the system requirements for the installation or upgrade.
7. From the Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** section, press **Enter**.  
The **System Information** section appears.
8. Type the absolute path for the installation directory.  
The directory names in the path must not contain spaces or the following special characters: @|\* \$ # ! % ( ) { } [ ] , ; '
 

**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
9. Press **Enter**.
10. Enter the starting port number for the node that you will create or upgrade on the machine. The default port number for the node is 6005.
11. Press **Enter**.  
The **Database and Connection Information** section appears.
12. To enter the JDBC connection information using a custom JDBC connection string, press **1**. To enter the JDBC connection information using the JDBC URL information, press **2**.  
To connect to a secure database, you must enter the JDBC connection using a custom JDBC connection string.
13. Enter the JDBC connection information.
  - To enter the connection information using a custom JDBC connection string, type the connection string and specify the connection parameters.  
Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

### Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

### Azure SQL Database with Active Directory authentication

```
jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

### Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the connection information:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following database types: <ul style="list-style-type: none"><li>- 1 - Oracle</li><li>- 2 - Microsoft SQL Server</li><li>- 3 - IBM DB2</li><li>- 4 - Sybase ASE</li><li>- 5 - PostgreSQL</li></ul>
Database user ID	User ID for the database user account for the domain configuration repository.
Database user password	Password for the database user account.
Database host name	Host name for the database server.
Database port number	Port number for the database.
Database service name	Service name for Oracle and IBM DB2 databases, or database name for PostgreSQL, Microsoft SQL Server, and Sybase ASE.

- To connect to a secure database, select **1** to use a custom string and type the connection string. You must include the security parameters in addition to the connection parameters. For information about the security parameters you must include in the JDBC connection for a secure database, see [“Connection String to a Secure Database” on page 96](#).

The tool checks the settings of the hard drive, the availability of the ports, and the configuration of the database. After the system check is complete, the **System Check Summary** section displays the results of the system check.

14. Analyze the results of the system check.

Each requirement is listed, along with one of the following check statuses:

- [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
- [Fail] - The requirement doesn't meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
- [Information] - Verify the information and perform any additional tasks as outlined in the details.

The results of the system check are saved to the following file: ...<Informatica installation directory>/Server/I10PI/I10PI/en/I10PI\_summary.txt

15. Press **Enter** to close the Pre-Installation (i10Pi) System Check Tool.

You can continue to the Informatica service installation or upgrade immediately or end the system check and continue with the installation or upgrade later. If you continue to the installation or upgrade immediately, you do not have to restart the installer.

16. To continue to the Informatica service installation or upgrade immediately, press **y**.

To end the system check and continue with the installation or upgrade later, press **n**.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.



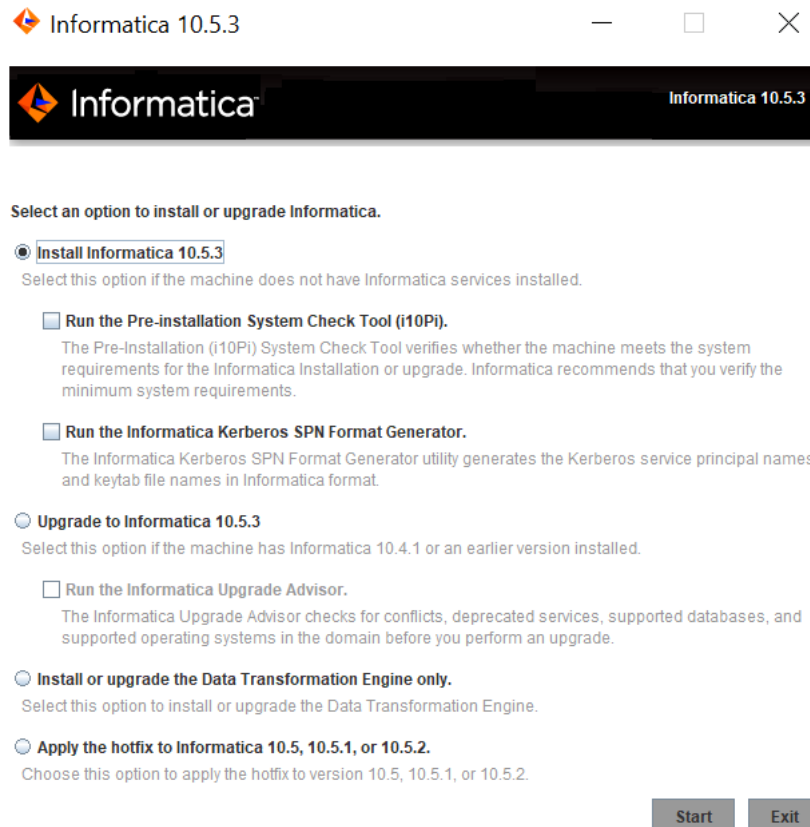
**Note:** If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

## Run the Pre-Installation (i10Pi) System Check Tool in Graphical Mode

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation or upgrade.

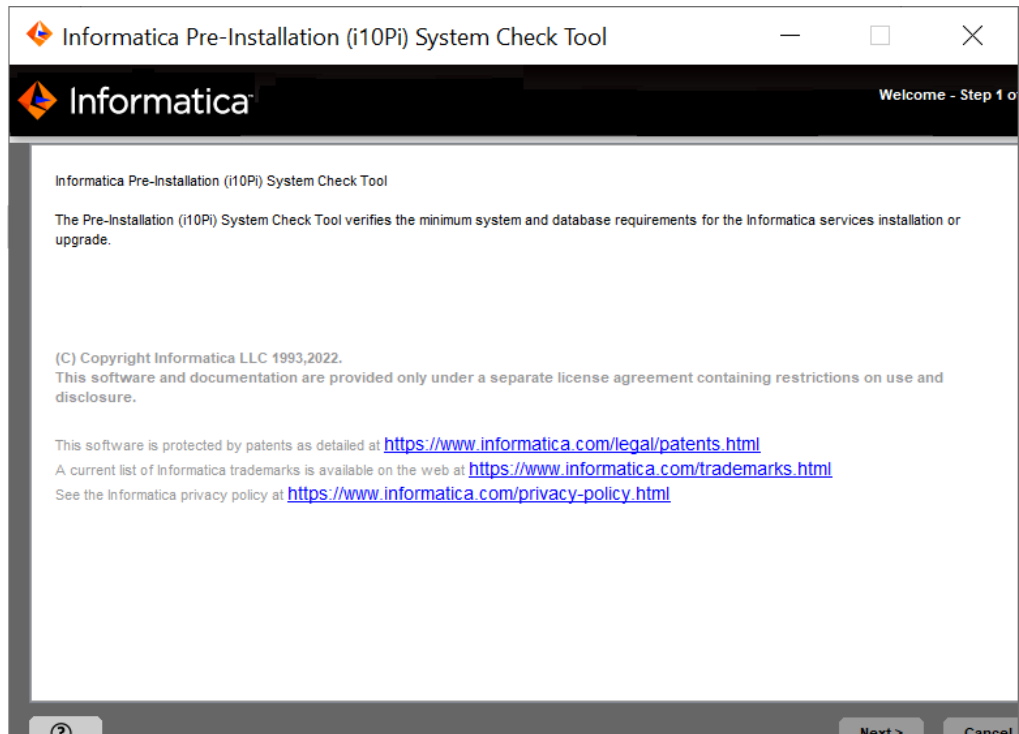
Ensure that you verified the system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Go to the root of the directory that contains the installation files and run install.bat as administrator.
4. Select **Install Informatica 10.5.3**.
5. Select **Run the Pre-Installation (i10Pi) System Check Tool** to verify whether the machine meets the system requirements for the installation or upgrade.



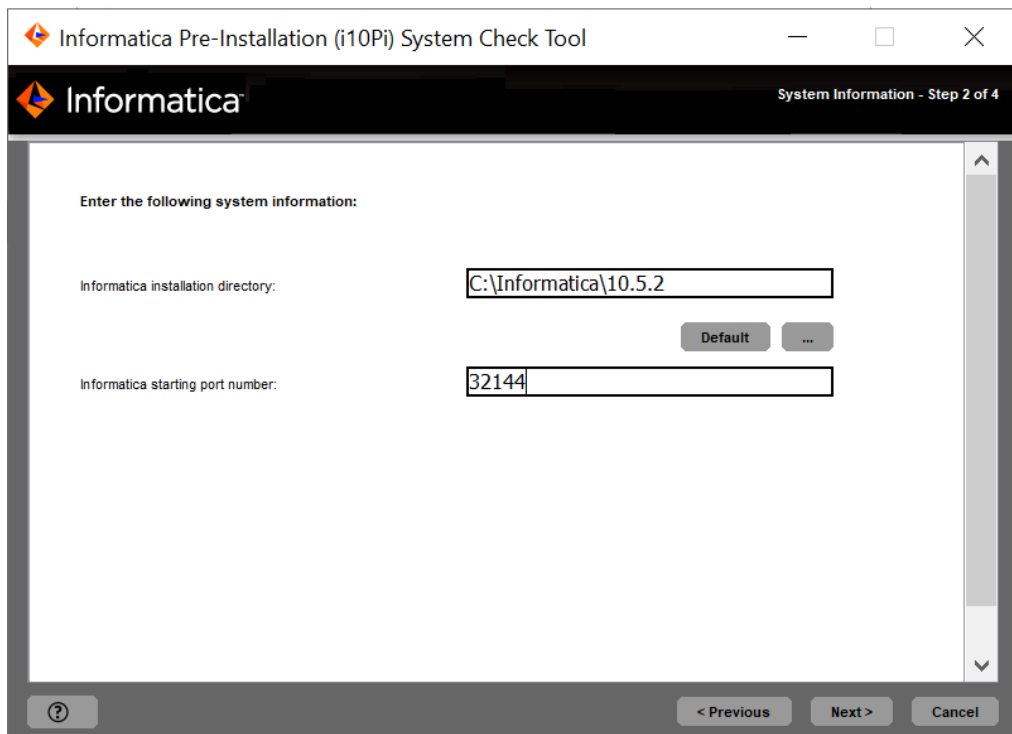
6. Click **Start**.

The Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** page appears.



7. Click **Next**.

The **System Information** page appears.



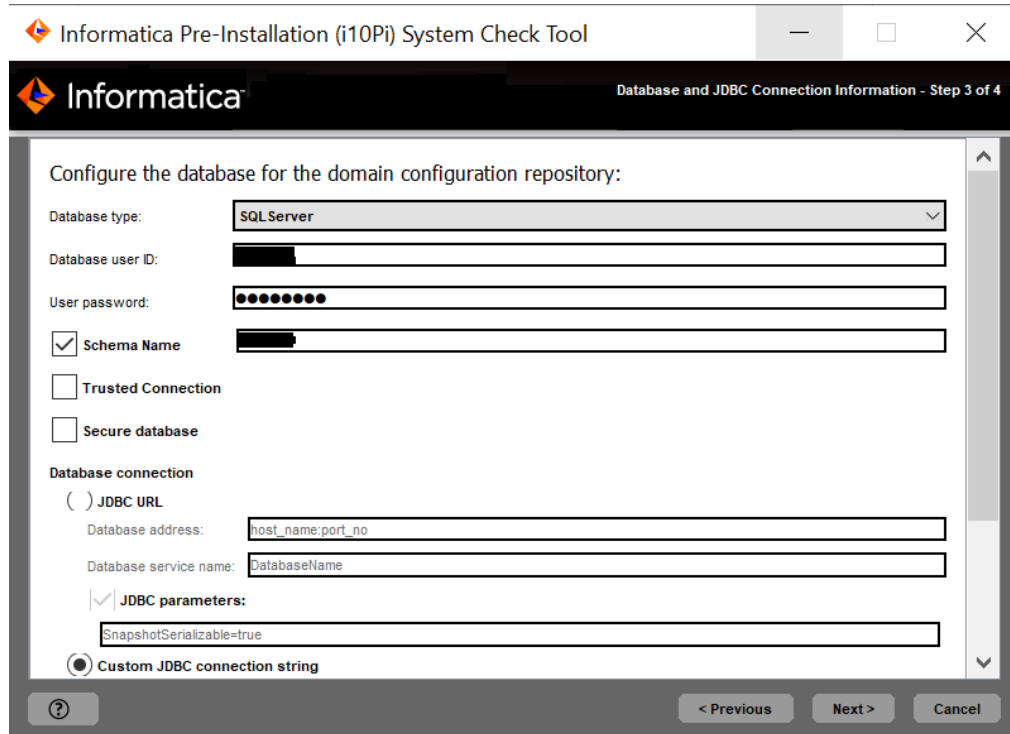
8. Enter the absolute path for the installation directory.

The directory names in the path must not contain spaces or the following special characters: @ | \* \$ # ! % ( ) { } [ ] , ; ' .

**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

9. Enter the starting port number for the node that you will create or upgrade on the machine. The default port number for the node is 6005.
10. Click **Next**.

The **Database and JDBC Connection Information** page appears.



11. Enter the information for the domain configuration repository database.  
The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: <ul style="list-style-type: none"><li>- Oracle</li><li>- IBM DB2</li><li>- Microsoft SQL Server</li><li>- PostgreSQL</li><li>- Sybase ASE</li></ul>
Database user ID	User account for the repository database.
User password	Password for the database user account.

The domain configuration repository must be accessible to all gateway nodes in the domain.

12. If you plan to use a secure database for the domain configuration repository, select the **Secure database** option.

13. Enter the database connection information.

- To enter the connection information using the JDBC URL information, select **JDBC URL** and specify the JDBC URL properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format <code>host_name:port</code> .
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- Sybase ASE: Enter the database name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

Use the following syntax in the JDBC connection string:

**IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

**Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

**Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

**Microsoft SQL Server with Windows NT credentials**

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

### Azure SQL Database with Active Directory authentication

```
jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

### Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

- If you select the **Secure database** option, select **Custom JDBC connection string** and type the connection string.  
You must include the security parameters in addition to the connection parameters. For information about the security parameters you must include in the JDBC connection for a secure database, see ["Connection String to a Secure Database" on page 96](#).

14. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.

15. Click **Next** to start the system check.

The tool checks the settings of the hard drive, the availability of the ports, and the configuration of the database. After the system check is complete, the **System Check Summary** page appears, displaying the results of the system check.

16. Analyze the results of the system check.

Each requirement is listed, along with one of the following check statuses:

- [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
- [Fail] - The requirement doesn't meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
- [Information] - Verify the information and perform any additional tasks as outlined in the details.

The results of the system check are saved to the following file: ...<Informatica installation directory>/Server/I10PI/I10PI/en/I10PI\_summary.txt

17. Click **Done** to close the Pre-Installation (i10Pi) System Check Tool.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

**Note:** If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

# Run the Pre-Installation (i10Pi) System Check Tool in Silent Mode

Run the Pre-installation (i10Pi) System Check Tool in silent mode to verify system requirements for installation without user intervention.

1. Extract the Informatica services installer file.
2. Navigate to the following location:  
`<Informatica installation directory>/Server/I10PI`
3. To specify the properties for the I10PI system check tool in silent mode, update the `SilentInput.properties` file in the I10PI folder.
4. To run the i10Pi in silent mode, run the `silentInstall` file in the I10PI folder.

You can view the results of the i10Pi system check tool in silent mode from the `I10PI_summary.txt` file in the following location:

`<Informatica installation directory>/Server/I10PI/I10PI/en`

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

**Note:** If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

# Part III: Run the Services Installer

This part contains the following chapters:

- [Install Informatica Services in Console Mode, 112](#)
- [Install Informatica Services in Graphical Mode, 157](#)
- [Run the Silent Installer, 231](#)
- [Troubleshooting , 234](#)

## CHAPTER 8

# Install Informatica Services in Console Mode

This chapter includes the following topics:

- [Informatica Services Installation Overview, 112](#)
- [Create a Domain, 112](#)
- [Join a domain, 144](#)

## Informatica Services Installation Overview

You can install the Informatica services on multiple machines. The installation process creates a service named Informatica that runs as a daemon.

The first time you run the installer, you create a domain. If you are installing on multiple machines and you have created a domain, you join the domain.

When you create a domain, the node on the machine where you install becomes a gateway node in the domain. You can choose to set up secure communication between services within the domain. You can also choose to create some application services during the installation process.

When you join a domain, you can configure the node that you create to be a gateway node. When you create a gateway node, you can select enable a secure HTTPS connection to Informatica Administrator.

**Note:** When you run the installer in console mode, the words Quit, Help, and Back are reserved words. Do not use them as input text.

## Create a Domain

Create a domain if you are installing for the first time or if you want to administer nodes in separate domains.

### Run the Installer

Perform the following steps to run the installer:

1. Log in to the machine with a system user account.



2. Use the following command to clear the DISPLAY variable in the machine: `unset DISPLAY`
3. Close all other applications.
4. On a shell command line, run the `install.sh` file.  
The installer displays the message to verify that the locale environment variables are set.
5. If the environment variables are not set, press **n** to exit the installer and set them as required.  
If the environment variables are set, press **y** to continue.

## Welcome to the Informatica Installer

- ▶ Press **1** to run the installer.  
The installer displays different options based on the platform you are installing on.  
The following options appear:
  - a. Press **1** to run the Pre-Installation System Check Tool.  
For more information about running the Pre-Installation (i10Pi) System Check Tool, see [“Run the Pre-Installation \(i10Pi\) System Check Tool in Console Mode” on page 101](#).
  - b. Press **2** to run the Informatica Kerberos SPN Format Generator.  
For more information about running the Informatica Kerberos SPN Format Generator, see [“Running the SPN Format Generator ” on page 85](#).
  - c. Press **3** to run the installer.

The **Welcome** section appears.

## Welcome - Accept Terms and Conditions

- ▶ Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.
  - a. Press **1** if you do not want to accept the terms and conditions.
  - b. Press **2** to accept the terms and conditions.

The **Component Selection** sections appears.

## Component Selection

After you accept terms and conditions, you can install Informatica domain services.

1. Press **1** to install Informatica domain services.  
This option installs version 10.5.3 domain services and the application service binaries.
2. Choose whether you want to run the installer on a network that uses Kerberos authentication.
  - a. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.
  - b. Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.
3. Choose whether you want to install distribution packages through the Informatica installer.
  - Press **1** if you don't need distribution packages or if you want to install them later.
  - Press **2** if you want to install distribution packages through the installer.

Default is 1.

4. If you choose to install distribution packages, select one or more packages from the list that you want to install. Separate multiple packages with a comma.

Default is 1.

The **Installation Prerequisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

## License and Installation Directory

After you verify the installation prerequisites, you can specify the installation directory.

1. Enter the absolute path for the installation directory.

The directory names in the path must not contain spaces or the following special characters: @|\* \$ # ! % () {} [] , ; ' .

Default is the user home directory for the user that runs the Informatica installation.

**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Enter the path and file name of the Informatica license key and press **Enter**.
3. Specify the environment type associated with the Informatica services installation.
  - Press **1** to set Sandbox environment for a basic environment used for proof of concept with minimal users.
  - Press **2** to set Development environment for the design environment.
  - Press **3** to set Test environment for high volume processing that is closest to a production environment.
  - Press **4** to set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.

Default is 1 for Sandbox.

If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“Domain Selection” on page 116](#).

## Network Security - Service Principal Level

After you specify the installation directory, you can configure security level.

- In the **Service Principal Level** section, select the level at which to set the Kerberos service principals for the domain.

**Note:** All nodes in the domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

The following table describes the levels that you can select:

Level	Description
Process Level	<p>Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node.</p> <p>The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.</p>
Node Level	<p>Configures the domain to share SPNs and keytab files on a node.</p> <p>This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node.</p> <p>Use the node level option for domains that do not require a high level of security, such as test and development domains.</p>

The **Network Security - Kerberos Authentication** section appears.

## Network Security - Kerberos Authentication

After you configure the security level, you can configure Keberos authentication.

- In the **Network Security - Kerberos Authentication** section, enter the parameters required for Kerberos authentication.

The following table describes the Kerberos authentication parameters that you must set:

Property	Description
Domain name	<p>Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , &lt; &gt; \ /</p>
Node name	Name of the Informatica node.
Node host name	<p>Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character.</p> <p><b>Note:</b> Do not use <i>localhost</i>. The host name must explicitly identify the machine.</p>
Service realm name	<p>Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase.</p> <p>The service realm name and the user realm name must be the same.</p>
User realm name	<p>Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase.</p> <p>The service realm name and the user realm name must be the same.</p>

Property	Description
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Fully qualified path to the kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i>

**Important:** If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

The **Pre-Installation Summary** section appears. Review the installation information.

## Domain Selection

After you review the Pre-Installation summary, you can enter the domain information.

1. Press **1** to create a domain.

When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.

2. Select whether you want to enable secure communication for services in the domain.

- a. Press **1** to disable secure communication for the domain.

- b. Press **2** to enable secure communication for the domain.

By default, if you enable secure communication for the domain, the installer sets up an HTTPS connection for the Informatica Administrator. You can also create a domain configuration repository on a secure database.

3. Specify the connection details for Informatica Administrator.

- a. If you do not enable secure communication for the domain, you can specify whether to set up a secure HTTPS connection for the Informatica Administrator.

The following table describes the options available to enable or disable a secure connection to Informatica Administrator:

Option	Description
Enable HTTPS for Informatica Administrator	Set up a secure connection to Informatica Administrator.
Disable HTTPS	Do not set up a secure connection to Informatica Administrator.

- b. If you enable secure communication for the domain or if you enable HTTPS connection for the Informatica Administrator, enter the keystore file and port number for the HTTPS connection to Informatica Administrator.

The following table describes the connection information you must enter if you enable HTTPS:

Option	Description
Port	Port number for the HTTPS connection.
Keystore file	<p>Select whether to use a keystore file generated by the installer or a keystore file you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.</p> <p>1 - Use a keystore generated by the installer 2 - Specify a keystore file and password</p> <p>If you select to use a keystore file generated by the installer, the installer creates a self-signed keystore file named Default.keystore in the following location: &lt;Informatica installation directory&gt;/tomcat/conf/</p>

- c. If you specify the keystore, enter the password and location of the keystore file.
  - d. If you enabled secure communication for the domain, the **Domain Security - Secure Communication** section appears.
  - e. If you did not enable secure communication for the domain, the **Domain Configuration Repository** section appears. Skip to ["Domain Configuration Repository" on page 120](#).
4. Select whether to enable SAML authentication to configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain.  
Press **1** to disable SAML authentication and skip to ["Domain Security - Secure Communication" on page 119](#). Press **2** to enable and configure SAML authentication.
  5. Enter the Identity Provider URL for the domain.
  6. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you choose No, the service provider identifier is set to "Informatica".
  7. Specify whether IdP will sign SAML assertion or not.
  8. Enter the identity provider assertion signing certificate alias name.
  9. Select whether to use the default Informatica SSL certificates or to use your SSL certificates to enable SAML authentication in the domain.

The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

10. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	Specify the directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

11. To specify the Authentication Context Comparison, specify the strength comparison of the authentication mechanism used by the user with the IdP server.  
Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.
12. To set the Authentication Context Class, specify the expected mechanism of first time authentication of the user with the IdP server.  
Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.
13. Specify if you want to enable the webapp to sign the SAML authentication request or not?  
Default is disabled.
14. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
15. Specify the password to access the private key used for signing the SAML request.
16. Specify the algorithm that the web application uses to sign the SAML request.  
Supported values are RSA\_SHA256, DSA\_SHA1, DSA\_SHA256, RSA\_SHA1, RSA\_SHA224, RSA\_SHA384, RSA\_SHA512, ECDSA\_SHA1, ECDSA\_SHA224, ECDSA\_SHA256, ECDSA\_SHA384, ECDSA\_SHA512, RIPEMD160, or RSA\_MD5.
17. Specify whether you want IdP to sign the SAML response or not?  
Choose to select to enable the webapp to receive the signed SAML response or not. Default is disabled.
18. Specify whether IdP will encrypt SAML assertion or not.  
Select to enable the webapp to receive an encrypted SAML assertion. Default is enabled.
19. Specify the alias name of the private key present in the gateway nodes gateway node SAML truststore that used for Informatica uses to decrypt decrypting the SAML assertion.
20. Provide the password to access the private key to use when decrypting the assertion encryption key.
21. Click **Next**.

The **Domain Security - Secure Connection** section appears.

## Domain Security - Secure Communication

After you configure the domain, you can configure domain security.

- In the Domain Security - Secure Communication section, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure domain communication.

- a. Select the type of SSL certificates to use.

The following table describes the options for the SSL certificates that you can use to secure the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	Use the default SSL certificates contained in the default keystore and truststore. <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Specify the path for the keystore and truststore files that contain the SSL certificates. You must also specify the keystore and truststore passwords. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

- b. If you provide the SSL certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

The **Domain Configuration Repository** section appears.

## Domain Configuration Repository

After you configure domain security, you can configure domain repository details.

1. Select the database to use for the domain configuration repository details.

The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - Sybase ASE 5 - PostgreSQL

The Informatica domain configuration repository stores metadata for domain operations and user authentication. The domain configuration repository must be accessible to all gateway nodes in the domain.

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the domain configuration database user account.
User password	Password for the domain configuration database user account.

3. Select whether to create a secure domain configuration repository.

You can create a domain configuration repository in a database secured with the SSL protocol. To create a domain configuration repository in a secure database, press 1 and skip to step to create a domain configuration repository.

To create a domain configuration repository in an unsecure database, press 2.

4. If you do not create a secure domain configuration repository, enter the parameters for the database.
  - a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.



The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.

The following table describes the properties that you must configure for the database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.
- d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name. - PostgreSQL: Enter the database name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No  If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

#### IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

### Azure SQL Database with Active Directory authentication

```
jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

### Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

5. If you create a secure domain configuration repository, enter the parameters for the secure database. If you create the domain configuration repository on a secure database, you must provide the truststore information for the database.

The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

In addition to the host name and port number for the database server, you must include the following secure database parameters:

#### EncryptionMethod

Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to `SSL`.

#### ValidateServerCertificate

Optional. Indicates whether Informatica validates the certificate that the database server sends.

If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the `HostNameInCertificate` parameter, Informatica also validates the host name in the certificate.

If this parameter is set to False, Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify

Default is True.

#### **HostNameInCertificate**

Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.

#### **cryptoProtocolVersion**

Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server.

You must also provide a JDBC connection string that includes the security parameters for the database. You can use the following syntax for the connection strings:

- **Oracle:** `jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **IBM DB2:** `jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **Microsoft SQL Server:** `jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **Microsoft SQL Server with Windows NT credentials:**  
If you have previously specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.
  - Microsoft SQL Server that uses the default instance with Windows NT credentials:  
`"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"`
  - Microsoft SQL Server that uses a named instance with Windows NT credentials:  
`"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"`

- **Microsoft Azure SQL:** jdbc:Informatica:sqlserver://<host name:port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **PostgreSQL:** jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **Azure PostgreSQL:** jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;

**Note:** The installer does not validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

6. If the database contains a domain configuration repository for a previous domain, select to overwrite the data or set up another database.
  - a. Press 1 for OK to enter the connection information for a new database.
  - b. Press 2 for Continue for the installer to overwrite the data in the database with new domain configuration.

The **Domain Security - Encryption Key** section appears.

## Domain Security - Encryption Key

After you configure domain repository, you can configure encryption key.

- In the **Domain Security - Encryption Key** section, enter the directory for the encryption key for the Informatica domain.

The following table describes the encryption key parameters that you must specify when you create a domain:

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: <Informatica installation directory>/isp/config/keys.
Specify if you want to back up the site key that the installer generates or not	<p>A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.</p> <p>Specify if you want to back up the site key that the installer generates or not:</p> <ul style="list-style-type: none"> <li>- Select <b>1</b> for No. If you choose No, the installer generates an error. Press <b>Enter</b> to continue.</li> <li>- Select <b>2</b> for Yes. If you choose Yes, you agree to back up the file manually.</li> </ul>

The installer sets different permissions to the directory and the files in the directory. For more information about the permissions for the encryption key file and directory, see [“Secure Files and Directories” on page 100](#).

The **Domain and Node Configuration** section appears.

## Domain and Node Configuration

After you configure the encryption key, you can configure the domain and node.

1. Enter the information for the domain and the node that you want to create.

The following table describes the properties that you set for the domain and gateway node.

Property	Description
Domain name	<p>Name of the Informatica domain to create. The default domain name is Domain_&lt;MachineName&gt;.</p> <p>The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , &lt; &gt; \ /</p>
Node name	<p>Name of the node to create.</p>
Node host name	<p>Host name or IP address of the machine on which to create the node.</p> <p>If the machine has a single network name, use the default host name. If the a machine has multiple network names, you can modify the default host name to use an alternate network name.</p> <p><b>Note:</b> The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.</p>
Node port number	<p>Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.</p>
Domain user name	<p>User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines:</p> <ul style="list-style-type: none"><li>- The name is not case sensitive and cannot exceed 128 characters.</li><li>- The name cannot include a tab, newline character, or the following special characters: % * + / ? ; &lt; &gt;</li><li>- The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.</li></ul>

2. Select whether you want to enable password complexity to secure sensitive data in the domain.

The following table describes the password complexity:

Property	Description
Password complexity	<p>Select whether you want to enable password complexity.</p> <p>1 - Yes</p> <p>2 - No</p> <p>If you select Yes, the password must meet the following requirements:</p> <p>It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.</p>
Configure password policy	<p>Select whether you want to configure a password policy.</p> <p>1 - Yes</p> <p>2 - No</p> <p>If you select Yes, you can configure password complexity rules.</p> <p>If you select No, the default Informatica password policy rules apply.</p>
Number of special characters	<p>The minimum number of special characters required in a password.</p> <p>You can use the following special characters: [ ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~ ]</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Number of alphabetic characters	<p>The minimum number of alphabetic characters required in a password.</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Number of numeric characters	<p>The minimum number of numeric characters required in a password.</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Minimum password length	<p>The minimum number of characters required in a password.</p> <p>You can enter a value between 8 and 255. Default is 8.</p>
Number of previous passwords to store	<p>The number of consecutive previous passwords that can't be reused.</p> <p>You can enter a value between 0 and 12. Default is 0.</p>
Password expiration in days	<p>The duration of the validity of a password.</p> <p>If you don't want passwords to expire, set the value to 0. Default is 0.</p>
Domain password	<p>Password for the domain administrator.</p> <ul style="list-style-type: none"> <li>- If you don't enable password complexity, the password must be between 2 and 16 characters.</li> <li>- If you enable password complexity, the password must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.</li> <li>- If you configure a password policy, the password must meet the complexity rules that you set.</li> </ul> <p>Not available if you configure the Informatica domain to run on a network with Kerberos authentication.</p>
Confirm password	<p>Enter the password again to confirm.</p> <p>Not available if you configure the Informatica domain to run on a network with Kerberos authentication.</p>

3. Select whether to display the default ports for the domain and node components assigned by the installer.

The following table describes the advanced port configuration page:

Prompt	Description
Display advanced port configuration page	Select whether to display the port numbers for the domain and node components assigned by the installer: 1 - No 2 - Yes  If you select Yes, the installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.

4. If you display the port configuration page, enter new port numbers at the prompt or press Enter to use the default port numbers.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

5. Select if you want to configure the services and connection.

If you select Yes, you can configure the Model Repository Service, Data Integration Service, Content Management Service, PowerCenter Repository Service, and PowerCenter Integration Service, as well as the profiling warehouse connection and the connections associated with the cluster configuration.

If you select No, you can configure the application services from the Administrator tool.



If you choose to configure the services and connections, the **Configure Informatica application services** section appears. If you choose not to configure the services and connections, the **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## Configure Informatica Application Services

1. Select if you want to configure the Model Repository Service and Data Integration Service.
2. Select if you want to configure the monitoring Model Repository Service.
3. Select if you want to configure the Content Management Service.
4. Select if you want to configure the profiling warehouse connection.
5. Select if you want to create a Metadata Access Service. If the domain uses Kerberos authentication, don't choose to create the Metadata Access Service.
6. Select if you want to create a PowerCenter Repository Service and a PowerCenter Integration Service.

## Configure the Model Repository Database

After you configure the domain and the node, you can configure the Model repository database properties.

1. Enter the Model Repository Service name.

Enter the name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:

` ~ % ^ \* + = { } \ ; : ' " / ? . , < > | ! ( ) ] [

You cannot change the name of the service after you create it.

If you selected process level SPN, specify the Model Repository Service keytab file. The keytab file for the Model Repository Service process. The keytab file must have the following name: .keytab

2. Select the database to configure Model repository.

The following table lists the databases you can configure Model repository:

Prompt	Description
Database type	Type of database for the Model repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

3. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name of the Model repository database user account. You can enter the Windows NT user name for trusted connection on Microsoft SQL Server.
User password	Password for the Model repository user account. You can enter the Windows NT password for trusted connection on Microsoft SQL Server.

4. Select whether to create a secure Model repository database.

You can create a Model Repository Service in a database secured with the SSL protocol. To create a Model Repository Service in a secure database, press **1** and skip to step to enter the JDBC information.

To create a Model Repository Service in an unsecured database, press **2**.

5. If you chose not to create a secured Model repository, enter the parameters for the database.

- a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.

The following table describes the properties that you must configure for the database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	Service or database name : <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No  If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.  
Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### **Microsoft SQL Server with Windows NT credentials**

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

#### **Microsoft Azure SQL Database**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### **Azure SQL Database with Active Directory authentication**

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

#### **PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### **Azure PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

The **Service Parameters** section appears.

## Data Integration Service

After you configure the Model Repository database, you can configure the service parameters for the application services.

1. Enter the following service parameter information:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li><li>- HTTP&amp;HTTPS. Requests to the service can use either an HTTP or HTTPS connection.</li></ul>
HTTP port	Port number to use for the Data Integration Service. Default is 9085.
HTTPS port	Port number to use for the Data Integration Service. Default is 9085.

2. Select the SSL certificates to use to secure the Data Integration Service.

Option	Description
Use the default Informatica SSL certificate files	Use the default Informatica SSL certificates contained in the default keystore and truststore.  <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Use custom SSL certificates. You must specify the location of the keystore and truststore files.  You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

If you choose to use custom SSL certificates, enter the following information.

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

## Configure the Monitoring Model Repository Database

After you configure Model Repository database, you can configure the monitoring Model repository database properties.

1. Enter the monitoring Model Repository Service name.

Enter the name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:

`` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( ) ] [`

You cannot change the name of the service after you create it.

If you selected process level SPN, specify the monitoring Model Repository Service keytab file. The keytab file for the monitoring Model Repository Service process. The keytab file must have the following name: .keytab

2. Select the database type for the monitoring Model repository.

The following table lists the databases for the monitoring Model repository.

Prompt	Description
Database type	Type of database for the monitoring Model repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

3. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name of the monitoring Model repository database user account. You can enter the Windows NT user name for trusted connection on Microsoft SQL Server.
User password	Password for the monitoring Model repository user account. You can enter the Windows NT password for trusted connection on Microsoft SQL Server.

4. Select whether to create a secure monitoring Model repository database.

You can create a monitoring Model repository in a database secured with the SSL protocol. To create a monitoring Model repository in a secure database, press 1 and skip to step to enter the JDBC information.

To create a monitoring Model repository in an unsecured database, press 2.

5. If you do not create a secure monitoring Model repository, enter the parameters for the database.

- a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.

The following table describes the properties that you must configure for the database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. To enter the JDBC connection information using the JDBC URL information, press 1. To enter the JDBC connection information using a custom JDBC connection string, press 2.

d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	Service or database name : <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No  If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.



- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### **Microsoft SQL Server with Windows NT credentials**

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

#### **Microsoft Azure SQL Database**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### **Azure SQL Database with Active Directory authentication**

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

#### **PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### **Azure PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

The **Service Parameters** section appears.

## Content Management Service Parameters and Database

After you configure the Data Integration Service, you can configure the parameters for the Content Management Service.

1. Enter the following service parameter information:

Parameter	Description
Content Management Service name	Name of the Content Management Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Content Management Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li></ul>
HTTP port	Port number to use for the Content Management Service. Default is 8105.

2. If you select a keystore for the Content Management Service, enter the keystore file and port number for the HTTPS connection to the Content Management Service.

Select whether to use a keystore file generated by the installer or a keystore file you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.

- Use the default keystore generated by the installer.
- Specify the location and password of a custom keystore file.

If you select to use a keystore file generated by the installer, the installer creates a self-signed keystore file named Default.keystore in the following location: `<Informatica installation directory>/tomcat/conf/`

The keystore certificate types for the Content Management Service depends on the certificate types that the Administrator tool uses:

- If you used the default keystore certificate for the Administrator tool, you can use either the default or a custom keystore certificate for the Content Management Service.
- If you used a custom keystore certificate for the Administrator tool, you must use a custom keystore certificate for the Content Management Service.

3. Select the database type for the reference data warehouse.

The following table lists the databases for the reference data warehouse:

Prompt	Description
Database type	Type of database for the reference data warehouse. Select from the following options: <ul style="list-style-type: none"><li>- IBM DB2</li><li>- Microsoft Azure SQL Database</li><li>- Microsoft SQL Server</li><li>- Oracle</li><li>- PostgreSQL, using JDBC</li></ul>

4. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the reference data warehouse user account.
Database user password	Password for the reference data warehouse user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	<p>Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes.</p> <p>In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace.</p> <p>In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.</p>

5. To specify the schema name, press **1**. If you do not want to specify a schema name, press **2**. Default is **2**. If you select Microsoft SQL Server, specify the schema for the repository tables and database connection. If you do not specify a schema name, the installer creates the tables in the default schema.
6. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.
  - a. Enter the JDBC connection information.
    - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

#### IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

- Enter the data access connection string.

## Profiling Warehouse Database

After you configure the Content Management Service, you can you can configure the data profiling warehouse database.

1. Select the database type for the data profiling warehouse.

The following table lists the databases for the data profiling warehouse.

Prompt	Description
Database type	Type of database for the data profiling warehouse. Select from the following options: <ul style="list-style-type: none"><li>- Oracle</li><li>- Microsoft SQL Server</li><li>- IBM DB2</li></ul>

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the data profiling warehouse user account.
Database user password	Password for the data profiling warehouse user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

3. To specify the schema name, press **1**. If you do not want to specify a schema name, press **2**. Default is **2**. If you select Microsoft SQL Server, specify the schema for the repository tables and database connection. If you do not specify a schema name, the installer creates the tables in the default schema.
4. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	<p>Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes.</p> <p>In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace.</p> <p>In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.</p>

a. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	<p>Service or database name :</p> <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li></ul>
Configure JDBC Parameters	<p>Select whether to add additional JDBC parameters to the connection string:</p> <p>1 - Yes</p> <p>2 - No</p> <p>If you select Yes, enter the parameters or press Enter to accept the default.</p> <p>If you select No, the installer creates the JDBC connection string without parameters.</p>

- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### **Microsoft Azure SQL**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### **PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### **Azure PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

5. Enter the data access connection string.

## **PowerCenter Repository Service and PowerCenter Integration Service**

You can configure the PowerCenter Repository Service and the PowerCenter Integration Service.

1. Select the database to configure for the PowerCenter repository.

You can configure the PowerCenter repository with one of the following databases:

- 1 - Oracle
- 2 - Microsoft SQL Server
- 3 - PostgreSQL

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the PowerCenter repository database user account.
User password	Password for the PowerCenter configuration database user account.
Database service name	Service or database name for PowerCenter: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - PostgreSQL: Enter the database name.
Database host name	Enter the PowerCenter database host name .

3. Enter the name of the PowerCenter Repository Service to create.
4. Enter the name of the PowerCenter Integration Service to create.
5. Select the PowerCenter Repository Service code page. Default is 7-bit ASCII.
6. Select the PowerCenter Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## Join a domain

You can join a domain if you are installing on multiple machines and you have created a domain on another machine.

## Run the Installer

Perform the following steps to run the installer:

1. Log in to the machine with a system user account.
2. Use the following command to clear the DISPLAY variable in the machine: `unset DISPLAY`
3. Close all other applications.
4. On a shell command line, run the `install.sh` file.

The installer displays the message to verify that the locale environment variables are set.

5. If the environment variables are not set, press **n** to exit the installer and set them as required.  
If the environment variables are set, press **y** to continue.

## Welcome - Accept Terms and Conditions

- Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you



install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

- a. Press **1** to not accept the terms and conditions
- b. Press **2** to accept the terms and conditions.

If you choose to not accept the terms and condition, the installer prompts you to accept the terms and conditions.

The **Component Selection** section appears.

## Component Selection

After you accept terms and conditions, you can install Informatica domain services.

1. Press **1** to install Informatica domain services.  
This option installs version 10.5.3 domain services and the application service binaries.
2. Choose whether you want to run the installer on a network that uses Kerberos authentication.
  - a. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.
  - b. Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.
3. Choose whether you want to install distribution packages through the Informatica installer.
  - Press **1** if you don't need distribution packages or if you want to install them later.
  - Press **2** if you want to install distribution packages through the installer.Default is 1.
4. If you choose to install distribution packages, select one or more packages from the list that you want to install. Separate multiple packages with a comma.  
Default is 1.

The **Installation Prerequisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

## Installation Prerequisites

Verify the disk space and memory required for installation and complete the pre-installation tasks.

1. Verify that you have the required disk space and memory (RAM) available for installation.
2. Verify the database requirements for the domain configuration repository.
3. Complete the pre-installation tasks, including getting your Informatica license key, setting environment variables, and verifying port availability.

The **License and Installation Directory** section appears.

## License and Installation Directory

After you verify the installation prerequisites, you can specify the installation directory.

1. Enter the absolute path for the installation directory.

The directory names in the path must not contain spaces or the following special characters: @|\* \$ # ! % () {} [] , ; ' .

Default is the user home directory for the user that runs the Informatica installation.

**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Enter the path and file name of the Informatica license key and press **Enter**.
3. Specify the environment type associated with the Informatica services installation.
  - Press **1** to set Sandbox environment for a basic environment used for proof of concept with minimal users.
  - Press **2** to set Development environment for the design environment.
  - Press **3** to set Test environment for high volume processing that is closest to a production environment.
  - Press **4** to set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.

Default is 1 for Sandbox.

If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“Domain Selection” on page 147](#).

## Service Principal Level

After you specify the installation directory, you can configure security level.

- Select the level at which to set the Kerberos service principals for the domain.

**Note:** All nodes in the domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

The following table describes the levels that you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node.  The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node.  This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node.  Use the node level option for domains that do not require a high level of security, such as test and development domains.

The **Pre-Installation Summary** section appears. Press **Enter** to continue.

## Domain Selection

After you review the Pre-Installation summary, you can enter the domain information.

1. Press **2** to join a domain.

The installer joins a node on the machine where you install.

2. Specify whether the domain you want to join has the secure communication option enabled.

Press **1** to join an unsecure domain or press **2** to join a secure domain.

3. Select the type of node you want to create.

Press **1** to configure a gateway node or **2** to configure a worker node.

If you configure the node as a gateway, you can enable a secure HTTPS connection to the Informatica Administrator.

4. If you enable HTTPS connection for the Informatica Administrator, enter an HTTPS port number to use to secure the connection.

5. Select whether to use the default Informatica SSL certificates or to use your SSL certificates to enable SAML authentication in the domain.

The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

6. Select whether to enable Security Assertion Markup Language (SAML) authentication to configure SAML-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain.

Select if the domain uses SAML authentication:

- a. Press **1** for No to disable SAML authentication.

If you select No, skip to [“Domain Security - Secure Communication” on page 147](#).

- b. Press **2** for Yes to enable SAML authentication.

If you select Yes, configure the SAML authentication.

The **Domain Security - Secure Communication** appears.

## Domain Security - Secure Communication

After you select the domain, you can configure domain security.

- Specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure domain communication.

- a. Select the type of SSL certificates to use.

The following table describes the options for the SSL certificates that you can use to secure the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	Use the default SSL certificates contained in the default keystore and truststore. <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Specify the path for the keystore and truststore files that contain the SSL certificates. You must also specify the keystore and truststore passwords. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

- b. If you provide the SSL certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

The **Domain Configuration** section appears.

## Domain Configuration

After you configure domain security, you can configure domain repository connection details.

- Enter the information for the domain that you want to join.

The following table describes the properties that you specify for the domain:

Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.
Gateway node port	Port number of the gateway node.
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.
Security domain name	Name of the secure domain.

The **Domain Security - Encryption Key** section appears.

## Domain Security - Encryption Key

After you configure the domain repository, you can configure the encryption key.

- Enter the directory for the encryption key for the Informatica domain.

The following table describes the encryption key parameters that you must specify when you join a domain:

Prompt	Description
Select the encryption key	Path and file name of the encryption key for the Informatica domain that you want to join. All nodes in the Informatica domain use the same encryption key. You must specify the encryption key file created on the gateway node for the domain that you want to join. If you copied the encryption key file to a temporary directory to make it accessible to the nodes in the domain, specify the path and file name of the encryption key file in the temporary directory.
Encryption key directory	Directory in which to store the encryption key on the node created during this installation. The installer copies the encryption key file for the domain to the encryption key directory on the new node.

The installer sets different permissions to the directory and the files in the directory. For more information about the permissions for the encryption key file and directory, see [“Secure Files and Directories” on page 100](#).

The **Join Domain Node Configuration** section appears.

## Join Domain Node Configuration

After you configure the encryption key, you can configure the join domain and node.

1. Enter the information for the domain and the node that you want to join.

The following table describes the properties that you set for the current node.

Property	Description
Node host name	Host name or IP address of the machine on which to join the node. If the machine has a single network name, use the default host name. If the a machine has multiple network names, you can modify the default host name to use an alternate network name. <b>Note:</b> The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.
Node name	Name of the node to join.
Node port number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.

2. Select whether to display the advanced port configurations for the domain and node components assigned by the installer.  
  
If you select **1**, the installer does not display the port configurations. If you select **2** to create the ports, the **Port Configuration** section appears. The installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.
3. Select **1** to create the Model Repository Service and Data Integration Service through the installer. Select **2**to create them later.
4. Select **1** to create the PowerCenter Repository Service and the PowerCenter Integration Service through the installer. Select **2**to create them later.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## Port Configuration

If you chose to display the advanced port configuration page, you can set the ports for the domain components.

- Enter new port numbers at the prompt or press **Enter** to use the default port numbers.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

The **Post-Installation Summary** section appears. The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## Configure the Model Repository Database

After you configure the domain and the node, you can configure the Model repository database properties.

1. Enter the Model Repository Service name.

Enter the name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters:

` ~ % ^ \* + = { } \ ; : ' " / ? . , < > | ! ( ) ] [

You cannot change the name of the service after you create it.

If you selected process level SPN, specify the Model Repository Service keytab file. The keytab file for the Model Repository Service process. The keytab file must have the following name: .keytab

2. Select the database to configure Model repository.

The following table lists the databases you can configure Model repository:

Prompt	Description
Database type	Type of database for the Model repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

3. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name of the Model repository database user account. You can enter the Windows NT user name for trusted connection on Microsoft SQL Server.
User password	Password for the Model repository user account. You can enter the Windows NT password for trusted connection on Microsoft SQL Server.

4. Select whether to create a secure Model repository database.

You can create a Model Repository Service in a database secured with the SSL protocol. To create a Model Repository Service in a secure database, press **1** and skip to step to enter the JDBC information.

To create a Model Repository Service in an unsecured database, press **2**.

5. If you chose not to create a secured Model repository, enter the parameters for the database.

- a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.



The following table describes the properties that you must configure for the database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.
- d. Enter the JDBC connection information.
  - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	Service or database name : <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No  If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.  
Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### **Microsoft SQL Server with Windows NT credentials**

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

#### **Microsoft Azure SQL Database**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### **Azure SQL Database with Active Directory authentication**

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

#### **PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### **Azure PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

The **Service Parameters** section appears.

## Data Integration Service

After you configure the Model Repository database, you can configure the service parameters for the application services.

1. Enter the following service parameter information:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li><li>- HTTP&amp;HTTPS. Requests to the service can use either an HTTP or HTTPS connection.</li></ul>
HTTP port	Port number to use for the Data Integration Service. Default is 9085.
HTTPS port	Port number to use for the Data Integration Service. Default is 9085.

2. Select the SSL certificates to use to secure the Data Integration Service.

Option	Description
Use the default Informatica SSL certificate files	Use the default Informatica SSL certificates contained in the default keystore and truststore.  <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Use custom SSL certificates. You must specify the location of the keystore and truststore files.  You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

If you choose to use custom SSL certificates, enter the following information.

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

## PowerCenter Repository Service and PowerCenter Integration Service

You can configure the PowerCenter Repository Service and the PowerCenter Integration Service.

1. Select the database to configure for the PowerCenter repository.

You can configure the PowerCenter repository with one of the following databases:

- 1 - Oracle
- 2 - Microsoft SQL Server
- 3 - PostgreSQL

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the PowerCenter repository database user account.
User password	Password for the PowerCenter configuration database user account.
Database service name	Service or database name for PowerCenter: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - PostgreSQL: Enter the database name.
Database host name	Enter the PowerCenter database host name .

3. Enter the name of the PowerCenter Repository Service to create.
4. Enter the name of the PowerCenter Integration Service to create.
5. Select the PowerCenter Repository Service code page. Default is 7-bit ASCII.
6. Select the PowerCenter Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## CHAPTER 9

# Install Informatica Services in Graphical Mode

This chapter includes the following topics:

- [Install the Services in Graphical Mode Overview, 157](#)
- [Create a Domain, 157](#)
- [Join a Domain, 200](#)

## Install the Services in Graphical Mode Overview

You can install the Informatica services in graphical mode on Windows.

When you run the Pre-Installation (i10Pi) System Check Tool before you perform the installation, the installer sets the values for certain fields, such as the database connection and domain port numbers, based on the information you entered during the system check.

On Windows, if you encounter problems when you run the install.bat file from the root directory, run the following file: `<installer files directory>\server\install.exe`.

## Create a Domain

Create a domain if you are installing for the first time or if you want to administer nodes in separate domains.

### Run the Installer

Perform the following steps to run the installer:

1. Log in to the machine with a system user account.
2. Close all other applications.

3. Go to the root of the directory for the installation files and run install.bat as administrator.

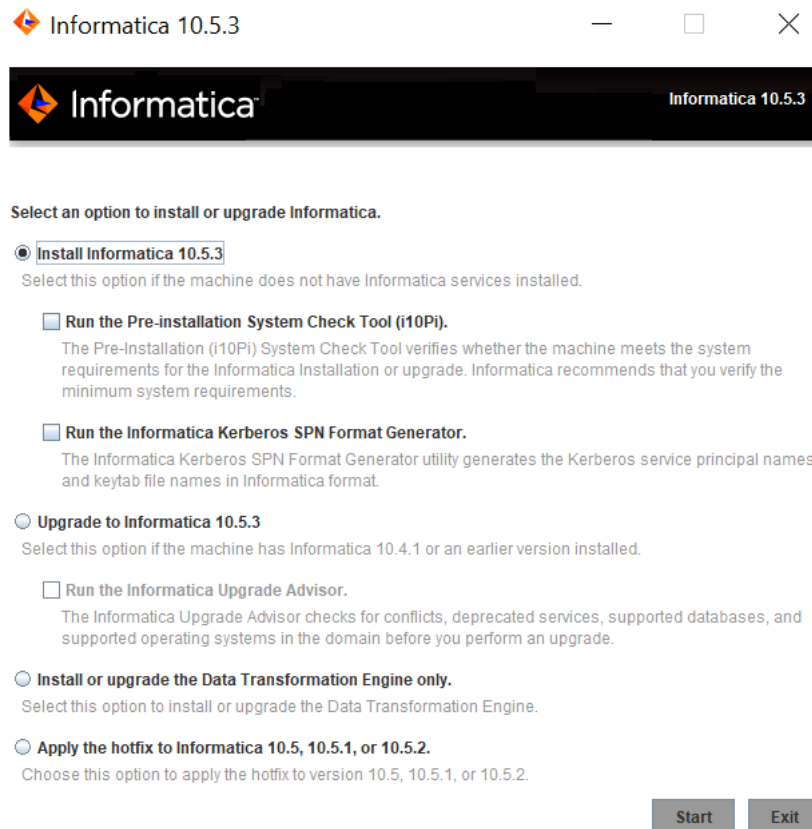
To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

**Note:** If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

The Informatica 10.5.3 page appears.

## Welcome to the Informatica Installer

1. Select **Install Informatica 10.5.3**.



Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

- Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

For more information about running the Pre-Installation (i10Pi) System Check Tool, see [“Run the Pre-Installation \(i10Pi\) System Check Tool in Graphical Mode” on page 105](#).

- Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

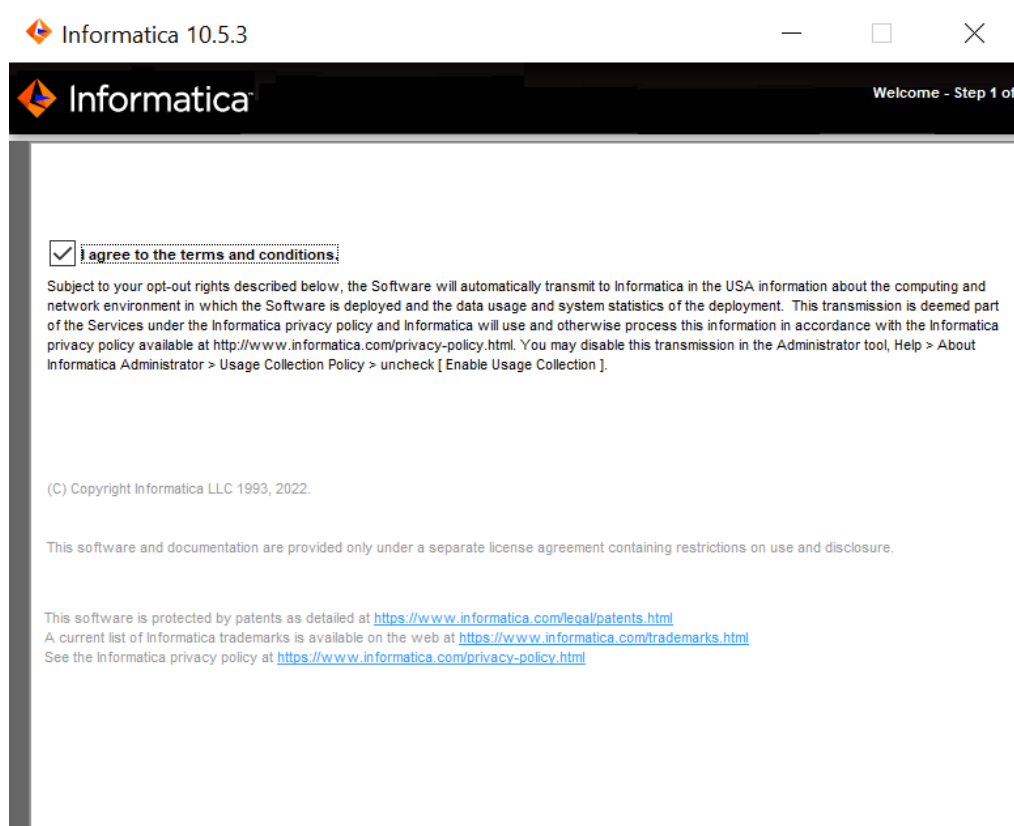
You can use the installer to run the utilities before you install informatica services. After you finish running a utility, restart the installer to run the next utility or install informatica services.

2. Click **Start**.

The **Welcome** section appears.

## Welcome - Accept Terms and Conditions

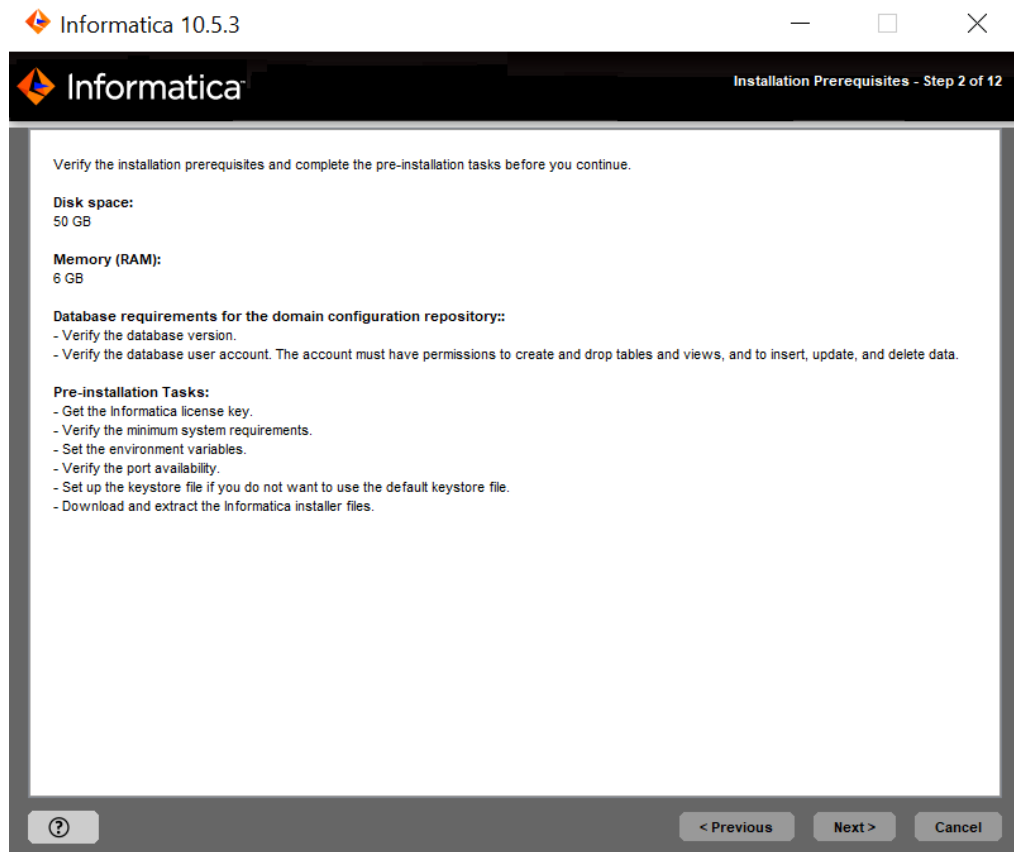
1. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.



Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

2. Click **Next**.

The **Installation Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.



3. Click Next.

The **License and Installation Directory** section appears.

## License and Installation Directory

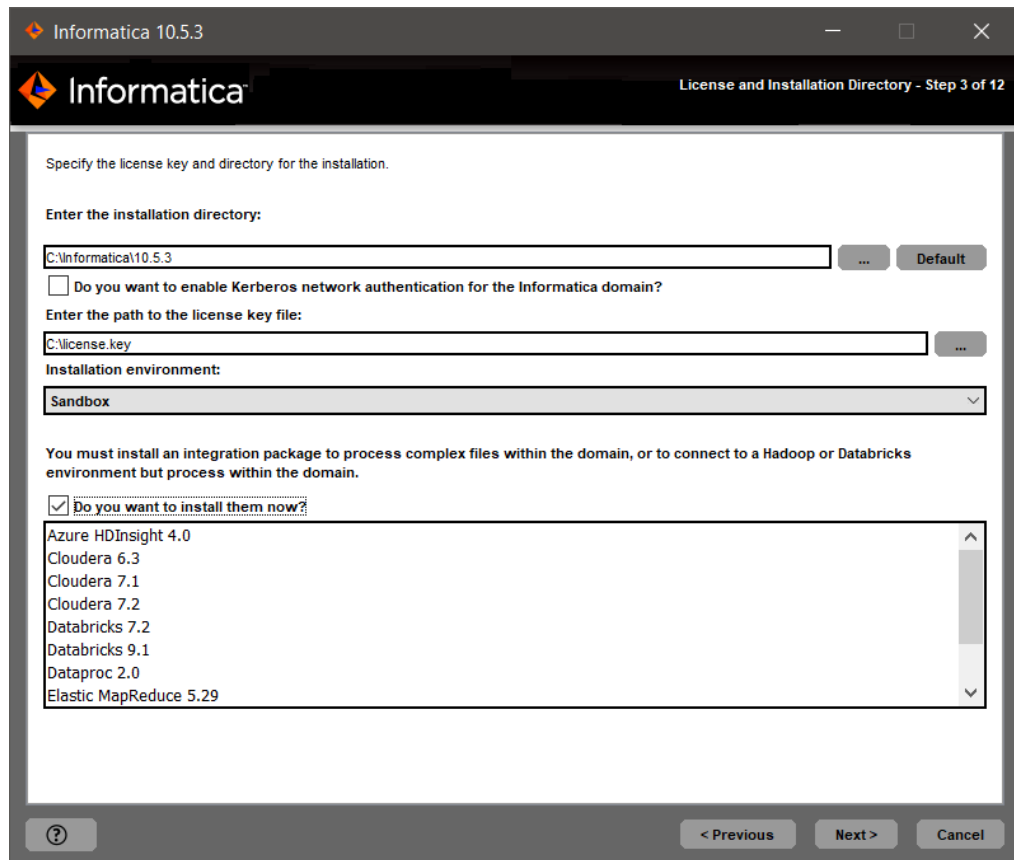
After you verify the installation prerequisites, you can specify the installation directory.

1. On the **License and Installation Directory** page, enter the Informatica license key, installation directory, installation environment, and distribution packages.



The following table describes the license key, directory that you specify for the Informatica services installation, and the distribution packages installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	<p>Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: @   * \$ # ! % ( ) { } [ ]</p> <p><b>Note:</b> Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.</p>
Installation environment	<p>Environment type associated with the Informatica services installation.</p> <ul style="list-style-type: none"> <li>- Set Sandbox environment for a basic environment used for proof of concept with minimal users.</li> <li>- Set Development environment for the design environment.</li> <li>- Set Test environment for high volume processing that is closest to a production environment.</li> <li>- Set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.</li> </ul>
Distribution packages	<p>You can choose whether to install distribution packages through the Informatica installer.</p> <p>If you choose to install distribution packages, select one or more packages from the list that you want to install.</p>



2. Click **Next**.

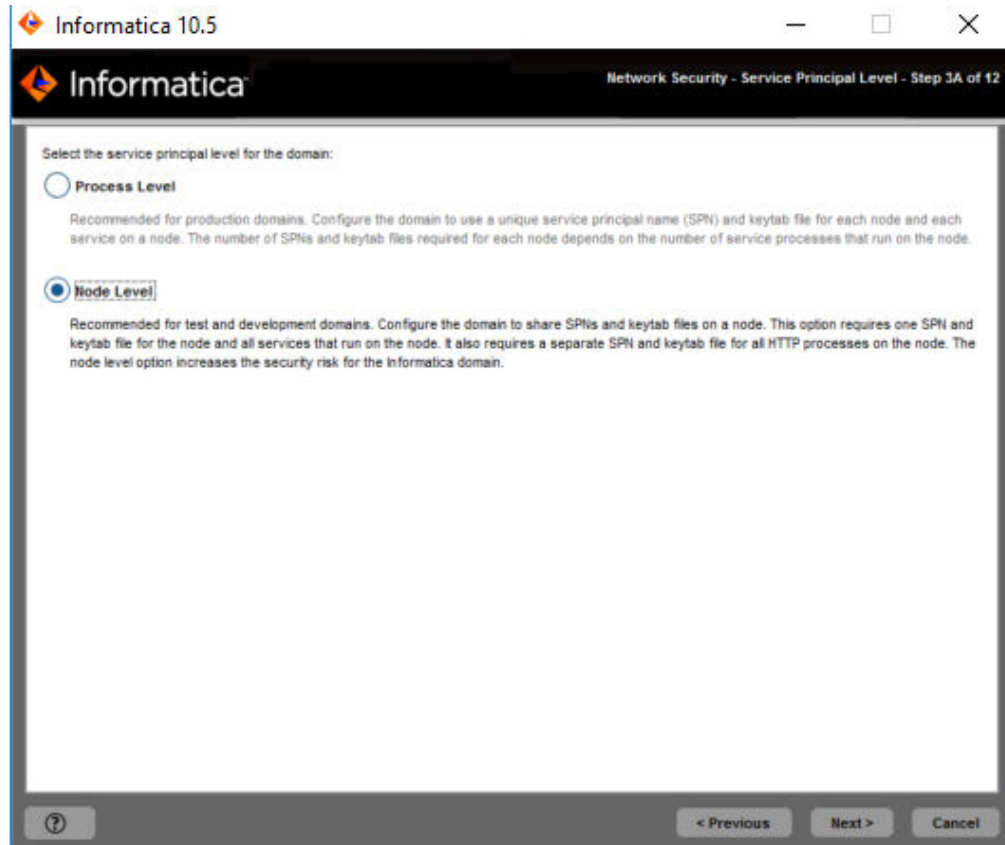
If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“Domain Selection” on page 116](#).

## Network Security - Service Principal Level

After you specify the installation directory, you can configure security level.

1. If you enable Kerberos network authentication, the **Network Security - Service Principal Level** appears.



2. On the **Network Security - Service Principal Level** page, select the level at which to set the Kerberos service principals for the domain.

The following table describes the service principal levels that you can select:

Level	Description
Process Level	<p>Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node.</p> <p>The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.</p>
Node Level	<p>Configures the domain to share SPNs and keytab files on a node.</p> <p>This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node.</p> <p>Use the node level option for domains that do not require a high level of security, such as test and development domains.</p>

3. Click **Next**.

The **Network Security - Kerberos Authentication** section appears.

# Network Security - Kerberos Authentication

After you configure the security level, you can configure Kerberos authentication.

- 1. The **Network Security - Kerberos Authentication** page, enter the domain and keytab information required for Kerberos authentication.

The following table describes the Informatica domain and node information that you must provide:

Property	Description
Domain name	Name of the domain to create. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the node to create.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. <b>Note:</b> The node host name cannot contain the underscore ( _ ) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	<p>Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive.</p> <p>To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example:</p> <p>*EAST.COMPANY.COM</p>
User realm name	<p>Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive.</p> <p>To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example:</p> <p>*EAST.COMPANY.COM</p>
Keytab directory	<p>Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.</p>
Kerberos configuration file	<p>Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i></p>

**Important:** If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

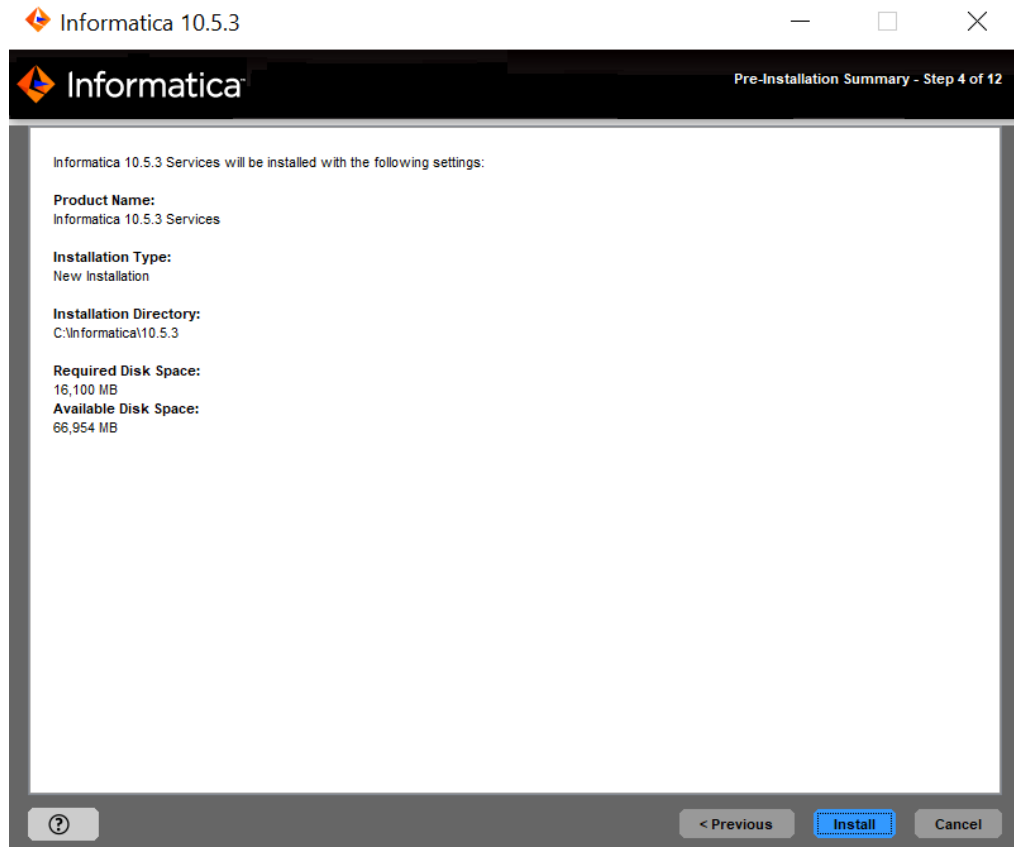
2. Click **Next**.

The **Pre-Installation Summary** section appears. Review the installation information.

## Domain Selection

After you review the Pre-Installation summary, you can enter the domain information.

1. Review the **Pre-Installation Summary** page.



2. Review the installation information, and click **Install** to continue.

The installer copies the Informatica files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

The screenshot shows the Informatica 10.5.3 Domain Selection - Step 5 of 12 window. The window has a dark header bar with the Informatica logo and the title "Domain Selection - Step 5 of 12". The main content area is white and contains the following options:

- Do you want to create a domain or join a domain?**
  - ☒ **Create a domain.**  
Create an Informatica domain if you are installing for the first time or if you are creating multiple domains.
    - ☒ **Do you want to enable secure communication for the domain?**
  - ☐ **Join a domain.**  
Join an Informatica domain on another node.
    - ☐ Do you want to join a secure domain?
    - ☐ Do you want this node to be a gateway node?
- ☒ **Enable HTTPS for Informatica Administrator.** Port:
- ☒ **Use the default keystore generated by the installer.**
- ☐ **Specify the location and password of a custom keystore file.**
  - Keystore password:
  - Keystore file:
- ☒ **Do you want to enable Security Assertion Markup Language (SAML) authentication?**

At the bottom of the window, there is a question mark icon on the left and "Next >" and "Cancel" buttons on the right.

3. Select **Create a domain**.  
When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.
4. Select the checkbox to enable secure communication between services in the domain.  
By default, if you enable secure communication for the domain, the installer sets up an HTTPS connection for the Informatica Administrator. You can also create a domain configuration repository on a secure database.
5. To secure the connection to Informatica Administrator, select **Enable HTTPS for Informatica Administrator**.

The following table describes the properties that you set for a secure connection to the Administrator tool:

Property	Description
Enable HTTPS for Informatica Administrator	Select this option to secure the connection to Informatica Administrator. To use an unsecure HTTP connection, clear the option.  By default, if secure communication is enabled for the domain, the installer enables this option. You can also enable this option even if you do not enable secure communication for the domain.
Port	The port to use for communication between Informatica Administrator and the Service Manager.
Use a keystore file generated by the installer	Use a self-signed keystore file generated by the installer. The installer creates a keystore file named Default.keystore in the following location: <Informatica installation directory>\tomcat\conf\
Specify a keystore file and password	Use a keystore file that you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.
Keystore password	A plain-text password for the keystore file. Required if you use a keystore file that you create.
Keystore file	Path and file name of the keystore file. Required if you use a keystore file that you create.

- To configure Security Assertion Markup Language (SAML) based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, select the checkbox to enable SAML authentication.

**Note:** If you enable Kerberos network authentication, you cannot configure SAML authentication.

- Click **Next**.



If you select the checkbox to enable SAML authentication option, the **SAML Authentication** page appears.

The screenshot shows the Informatica 10.5.3 SAML Authentication configuration window, Step 5A of 12. The window has a dark header bar with the Informatica logo and the text "SAML Authentication - Step 5A of 12". The main content area is white and contains the following fields and options:

- Identity Provider URL**: A text input field.
- ☒ **Do you want to enter a relying party trust name or a service provider identifier? If you choose No, the service provider identifier will be used.**
- Service Provider ID**: A text input field.
- ☒ **Enable SAML Assertion Signature Validation**
- SAML Assertion Signing Certificate Alias Name**: A text input field.
- Select the truststore for SAML authentication where you imported the identity provider assertion signing certificate**:
  - ☒ **Use the default Informatica truststore and keystore.**
  - ☐ **Use a custom truststore and keystore.**
- Specify the directory that contains the custom truststore to use for SAML authentication:**: A text input field.
- Specify the truststore password**: A text input field.
- Specify the directory that contains the custom keystore to use for SAML authentication:**: A text input field.
- Specify the keystore password**: A text input field.

At the bottom of the window, there is a navigation bar with a question mark icon, "< Previous", "Next >", and "Cancel" buttons.

**Informatica** SAML Authentication - Step 5A of 12

Specify the directory that contains the custom keystore to use for SAML authentication:

Specify the keystore password

**Authentication Context Comparison**

**Authentication Context Class**

☒ Enable SAML Request Signing Configuration

**SAML Request Signing Private Key Alias Name**

**SAML Request Signing Private Key Password**

**SAML Request Signing Algorithm**

☒ Enable SAML Response Signature Validation

**SAML Response Signing Certificate Alias Name**

☒ Enable SAML Assertion Encryption Configuration

**Encrypted Assertion Private Key Alias Name**

**Encrypted Assertion Private Key Password**

< ? < Previous Next > Cancel

8. Enter the Identity Provider URL for the domain.
9. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you choose No, the service provider identifier is set to "Informatica".
10. Specify whether IdP will sign SAML assertion or not.
11. Enter the identity provider assertion signing certificate alias name.
12. Specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

13. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	Specify the directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

14. To specify the Authentication Context Comparison, specify the strength comparison of the authentication mechanism used by the user with the IdP server.  
Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.
15. To set the Authentication Context Class, specify the expected mechanism of first time authentication of the user with the IdP server.  
Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.
16. Specify if you want to enable the webapp to sign the SAML authentication request or not?  
Default is disabled.
17. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
18. Specify the password to access the private key used for signing the SAML request.
19. Specify the algorithm that the web application uses to sign the SAML request.  
Supported values are RSA\_SHA256, DSA\_SHA1, DSA\_SHA256, RSA\_SHA1, RSA\_SHA224, RSA\_SHA384, RSA\_SHA512, ECDSA\_SHA1, ECDSA\_SHA224, ECDSA\_SHA256, ECDSA\_SHA384, ECDSA\_SHA512, RIPEMD160, or RSA\_MD5.
20. Specify whether you want IdP to sign the SAML response or not?  
Choose to select to enable the webapp to receive the signed SAML response or not. Default is disabled.
21. Specify whether IdP will encrypt SAML assertion or not.  
Select to enable the webapp to receive an encrypted SAML assertion. Default is enabled.
22. Specify the alias name of the private key present in the gateway nodes gateway node SAML truststore that used for Informatica uses to decrypt decrypting the SAML assertion.
23. Provide the password to access the private key to use when decrypting the assertion encryption key.
24. Click **Next**.

If you do not enable secure communication for the domain, the **Domain Configuration Repository** page appears. Skip to step that describes the Domain Configuration Repository page. If you selected the checkbox to enable secure communication for the domain, the **Domain Security - Secure Communication** page appears.

## Domain Security - Secure Communication

After you configure the domain, you can configure domain security.

1. On the **Domain Security - Secure Communication** page, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

The screenshot shows the Informatica 10.5.3 configuration window for Domain Security - Secure Communication, Step 5B of 12. The window title bar includes the Informatica logo and version number. The main content area has a black header bar with the Informatica logo and the title 'Domain Security - Secure Communication - Step 5B of 12'. Below the header, the text 'Select the SSL certificates to enable secure communication within the domain:' is displayed. There are two radio button options: 'Use the default Informatica SSL certificates contained in the default keystore and truststore.' (which is selected) and 'Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the c'. Below the second option, there are four input fields: 'Keystore file directory:' with 'c:\temp', 'Keystore password:', 'Truststore file directory:' with 'c:\temp', and 'Truststore password:'. At the bottom of the window, there is a navigation bar with a question mark icon, '< Previous', 'Next >', and 'Cancel' buttons.

Informatica 10.5.3

Domain Security - Secure Communication - Step 5B of 12

Select the SSL certificates to enable secure communication within the domain:

☒ Use the default Informatica SSL certificates contained in the default keystore and truststore.

☐ Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the c

Keystore file directory: c:\temp

Keystore password:

Truststore file directory: c:\temp

Truststore password:

< Previous Next > Cancel

The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	<p>Use the default SSL certificates provided by Informatica.</p> <p><b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.</p>
Use custom SSL certificates	<p>Specify the path of the keystore and truststore files that contain the SSL certificates.</p> <p>You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files.</p> <p>Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain.</p> <p>Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.</p> <p>To set the private truststore files, you must manually import the certificates. Run the keytool command in the &lt;INFA_JDK_HOME&gt; directory to import the private truststore certificates. For example, use the following keytool command:</p> <pre>keytool -noprompt -importkeystore -srckeystore &lt;source truststore file path&gt; -srcstorepass &lt;source truststore file password&gt; -srcalias &lt;alias&gt; -srcstoretype JKS -destkeystore &lt;destination truststore file path&gt; -deststorepass &lt;destination truststore file password&gt; -keypass &lt;private key password&gt; -deststoretype JKS</pre>

- If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

- Click **Next**.

The **Domain Configuration Repository** page appears.

## Domain Configuration Repository

After you configure domain security, you can configure domain repository details.

1. On the **Domain Configuration Repository** page, enter the database and user account information for the domain configuration repository.

Informatica 10.5.3

Domain Configuration Repository - Step 6 of 12

Enter database information for the domain configuration repository.

Database type: [ ]

Database user ID: [ ]

Database user password: [ ]

☐ Is the database secure?

Database connection

( ) Enter the JDBC URL.

Database address: [ ]

Database service name: [ ]

☒ JDBC parameters:

[ ]

(X) Enter the JDBC connection string.

[ ]

< Previous Next > Cancel

The domain configuration repository stores metadata for domain operations and user authentication. The database must be accessible to all gateway nodes in the domain.

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: <ul style="list-style-type: none"><li>- Oracle</li><li>- IBM DB2</li><li>- Microsoft SQL Server</li><li>- PostgreSQL</li><li>- Sybase ASE</li></ul>
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enabled secure communication for the domain, you can create the domain configuration repository in a database secured with the SSL protocol. Select the checkbox if you want to secure a database and skip to step [3](#).

**Note:** You cannot configure a secure connection to a Sybase database.

2. Enter the database connection information.

If you do not create a secure domain configuration repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

- To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format <code>host_name:port</code> .
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- Sybase ASE: Enter the database name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To connect using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.
3. If you choose to secure a database, enter the connection information using a custom JDBC connection string.

If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

For information about the security parameters you must include in the JDBC connection for a secure database, see [“Connection String to a Secure Database” on page 96](#).

4. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
5. Click **Next**.

The **Domain Security - Encryption Key** section appears.



## Domain Security - Encryption Key

After you configure domain repository, you can configure encryption key.

1. In the **Domain Security - Encryption Key** section, enter the encryption key parameters that you must specify when you create a domain.

The screenshot shows the 'Domain Security - Encryption Key' configuration window for Informatica 10.5.3, Step 7 of 12. The window title bar includes the Informatica logo and version. The main content area has a header 'Enter the encryption key information.' Below this, there is a section for 'Encryption key directory:' with a text box containing 'C:\Informatica\10.5.3\isp\config\keys' and a 'Default' button. A note states: 'A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not specify if you want to backup the site key that the installer generates or not.' Below the note is a checkbox labeled 'Do you agree?' which is checked. At the bottom of the window are navigation buttons: '< Previous', 'Next >', and 'Cancel'.

The following table describes the encryption key parameters that you must specify when you create a domain:

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: <Informatica installation directory>/isp/config/keys.
Specify if you want to back up the site key that the installer generates or not:	<p>A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.</p> <p>Specify if you want to back up the site key that the installer generates or not:</p> <ul style="list-style-type: none"><li>- Select 1 for No. If you choose No, the installer exits.</li><li>- Select 2 for Yes. If you choose Yes, you agree to back up the file manually.</li></ul>

The installer sets different permissions to the directory and the files in the directory. For more information about the permissions for the encryption key file and directory, see [“Secure Files and Directories” on page 100](#).

2. Click **Next**.

The **Domain and Node Configuration** section appears.

## Domain and Node Configuration

After you configure the encryption key, you can configure the domain and node.

1. Enter the information for the domain and the node that you want to create.

Informatica 10.5.3

Domain and Node Configuration - Step 8 of 12

Enter information for the Informatica domain.

Domain name:

Node host name:

Node name:

Node port number:

Domain user name:

☒ Do you want to enable password complexity?

☒ Do you want to configure password complexity?

Number of special characters (0 to 255):

Number of alphabetic characters (0 to 255):

Number of numeric characters (0 to 255):

Minimum password length (8 to 255):

Number of previous passwords to store (0 to 12):

Password validity (0 for infinite days):

Domain password:

Confirm password:

< Previous Next > Cancel

The following table describes the properties that you set for the domain and gateway node.

Property	Description
Domain name	Name of the Informatica domain to create. The default domain name is Domain_<MachineName>. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the node to create.

Property	Description
Node host name	<p>Host name or IP address of the machine on which to create the node.</p> <p>If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name.</p> <p><b>Note:</b> The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.</p>
Node port number	<p>Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.</p>
Domain user name	<p>User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines:</p> <ul style="list-style-type: none"> <li>- The name is not case sensitive and cannot exceed 128 characters.</li> <li>- The name cannot include a tab, newline character, or the following special characters: % * + / ? ; &lt; &gt;</li> <li>- The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.</li> </ul>

The following table describes the password complexity:

Prompt	Description
Password complexity	<p>Select whether you want to enable password complexity.</p> <p>If you select Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.</p>
Configure password policy	<p>Select whether you want to configure a password policy.</p> <p>If you select Yes, you can configure password complexity rules.</p> <p>If you select No, the default Informatica password policy rules apply.</p>
Number of special characters	<p>The minimum number of special characters required in a password.</p> <p>You can use the following special characters: [ ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` {   } ~ ]</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Number of alphabetic characters	<p>The minimum number of alphabetic characters required in a password.</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Number of numeric characters	<p>The minimum number of numeric characters required in a password.</p> <p>You can enter a value between 0 and 255. Default is 1.</p>
Minimum password length	<p>The minimum number of characters required in a password.</p> <p>You can enter a value between 8 and 255. Default is 8.</p>
Number of previous passwords to store	<p>The number of consecutive previous passwords that can't be reused.</p> <p>You can enter a value between 0 and 12. Default is 0.</p>

Prompt	Description
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.
Domain password	Password for the domain administrator. <ul style="list-style-type: none"> <li>- If you don't enable password complexity, the password must be between 2 and 16 characters.</li> <li>- If you enable password complexity, the password must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.</li> <li>- If you configure a password policy, the password must meet the complexity rules that you set.</li> </ul> Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

2. To display the default ports for the domain and node components assigned by the installer, enable **Display advanced port configuration page**.

If you display the port configuration page, the installer displays the default port numbers assigned to the domain and node. You can modify the port numbers or specify a different range of port numbers for the application service processes. If you do not select the display the port configuration page, the installer does not display the default port numbers and you cannot modify the assigned port numbers.

3. Select the checkbox to create the Model Repository Service and Data Integration Service during the installation.

If you do not configure the services, the installer does not create a Model Repository Service or a Data Integration Service in the new domain. You can create the services in the Administrator tool after installation.

If you select to configure the services, the installer creates a Model Repository Service and a Data Integration Service in the new domain. You must specify the database for the Model repository and configure the connection to the Data Integration Service. By default, the installer starts the services when the installation completes.

4. Choose whether to create a monitoring Model Repository Service to monitor domain statistics during installation.
5. Choose whether to create a Content Management Service for data domain discovery during installation.
6. Choose whether to configure the profiling warehouse connection during installation.
7. Choose whether to create a PowerCenter Repository Service and a PowerCenter Integration Service during the installation.

If you selected to display the port configuration page, the **Port Configuration** page appears.

If you do not select to display the port configuration page, the installer displays the **Windows Service Configuration** page.

## Port Configuration

You can update the port numbers for the Service Manager and Informatica Administrator.

1. If you selected to display the port configuration page, the **Port Configuration** page appears.

Informatica 10.5

Port Configuration - Step 8A of 12

Enter the port numbers for the Service Manager and Informatica Administrator.

Service Manager port: 20106

Service Manager shutdown port: 20107

Informatica Administrator port: 20108

Informatica Administrator shutdown port: 20109

Enter a range of port numbers for service processes in the node.

Minimum port number: 20114

Maximum port number: 20214

Default

< Previous Next > Cancel

2. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

Verify that the port numbers you enter are not used by other applications.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.

Port	Description
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

3. Click **Next**.

The **Windows Service Configuration** page appears.

## Windows Service Configuration

1. If you do not select to display the port configuration page, the installer displays the **Windows Service Configuration** page.

2. On the **Windows Service Configuration** page, select whether to run the Windows service under a different user account.

The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. Click **Next**.

If you do not choose to create the services, the installer displays the **Post-Installation Summary** page. The **Post-Installation Summary** page indicates whether the installation completed successfully.

If you select to configure the Informatica application services, the installer displays the **Model Repository Service Database** page.

## Configure Model Repository Service Database

After you configure the domain and the node, you can configure the Model repository database properties.

1. On the **Model Repository Service Database** page, enter the database and user account information for the Model repository.

Model Repository Service name:

Enter database information for the Model repository:

Database type:

Database user ID:

Database user password:

☐ Is the database secure?

Database connection

( ) Enter the JDBC URL.

Database address:

Database service name:

☒ JDBC parameters:

(●) Enter the JDBC connection string.

Next > Cancel

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: <ul style="list-style-type: none"> <li>- Oracle</li> <li>- IBM DB2</li> <li>- Microsoft SQL Server</li> <li>- PostgreSQL</li> </ul>
Database user ID	User account for the repository database.
User password	Password for the database user account.



If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enable secure communication for the domain, you can create the Model repository in a database secured with the SSL protocol. To create a secure Model repository, skip to step [3](#).

2. Enter the database connection information.

If you do not create a secure Model repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

- To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format <code>host_name:port</code> .
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

#### IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### Azure SQL Database with Active Directory authentication

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

#### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLV1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

3. Choose whether to create a secure Model repository.

If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

For information about the security parameters you must include in the JDBC connection for a secure database, see [“Connection String to a Secure Database” on page 96](#).

4. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
5. Click **Next**.

The **Service Parameters** section appears.

## Configure Monitoring Model Repository Service Database

After you configure Model Repository database, you can configure the monitoring Model repository database properties.

1. If you chose to create a monitoring Model Repository Service to monitor domain statistics, the **Model Repository Database for monitoring** page appears.

2. On the **Model Repository Database for monitoring** page, enter the database and user account information for the monitoring Model repository.

Property	Description
Database type	Database for the repository. Select one of the following databases: <ul style="list-style-type: none"> <li>- Oracle</li> <li>- IBM DB2</li> <li>- Microsoft SQL Server</li> <li>- PostgreSQL</li> </ul>
Database user ID	User account for the repository database. You can enter the Windows NT user name for trusted connection for Microsoft SQL Server.
User password	Password for the database user account. You can enter the Windows NT password for trusted connection for Microsoft SQL Server.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

3. Enter the database connection information.

You can specify the connection properties for the JDBC URL or provide the JDBC connection string.

- To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format <host name>:<port number>.
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

4. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.

5. Click **Next**.

The **Service Parameters** section appears.

# Data Integration Service

After you configure the Model Repository database, you can configure the service parameters for the application services.

1. On the **Data Integration Service** page, configure the Data Integration Service properties.

Informatica 10.5.3

Informatica Data Integration Service - Step 9C of 12

Enter a name for the Data Integration Service.

Data Integration Service name:

Enter the security properties:

Enter protocol for the Data Integration Service:

HTTPS port:

☒ Select the SSL certificates to secure the Data Integration Service:

☒ Use the default Informatica SSL certificates contained in the default keystore and truststore.

☐ Enter the location of the SSL certificate files.

Keystore file:

Keystore password:

Truststore file:

Truststore password:

Next > Cancel

The following table describes services parameters that you must set:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li><li>- HTTP&amp;HTTPS. Requests to the service can use either an HTTP or HTTPS connection.</li></ul>
HTTP port	Port number to used for the Data Integration Service. Default is 6030.

2. If you select an HTTPS connection, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure the connection to the Data Integration Service.

The following table describes the SSL certificate options for securing the Data Integration Service:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Enter the location of the SSL certificate files	Specify the path of the keystore and truststore files that contain the SSL certificates.

If you provide the certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name of the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.
Truststore file	Required. Path and file name of the truststore file that contains the public key for the database.
Truststore password	Required. Password for the truststore file for the secure database.

3. Click **Next**.

The installer creates the Data Integration Service.

## Content Management Service Parameters and Database

After you configure the Data Integration Service, you can configure the parameters for the Content Management Service.

1. If you chose to create a Content Management Service during the installation, the **Content Management Service** page appears.

Informatica 10.5.3

Content Management Service - Step 9D of 12

Enter reference data warehouse database information for the Content Management Service:

Database type:

Database user ID:

Database user password:

Data access connection string:

Configure the database connection:

☐ Enter the JDBC URL.

Database address:

Database service name:

☒ JDBC parameters:

☒ Enter the JDBC connection string.

< Previous Next > Cancel

2. Enter the Content Management Service parameters.

The following table describes the service parameters that you must set:

Port	Description
Content Management Service name	Name of the Content Management Service to create in the Informatica domain.
HTTP Protocol	Type of connection to the Content Management Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li></ul>
HTTP Port	Port number to use for the Content Management Service. Default is 8105.

3. If you select an HTTPS connection, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure the connection to the Content Management Service.



The following table describes the SSL certificate options for securing the Content Management Service:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Enter the location of the SSL certificate files	Use the SSL certificates that you provide. You must specify the location of the keystore files.

If you provide the certificate, specify the location and passwords of the keystore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name for the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.

The keystore certificate types for the Content Management Service depends on the certificate types that the Administrator tool uses:

- If you used the default keystore certificate for the Administrator tool, you can use either the default or a custom keystore certificate for the Content Management Service.
- If you used a custom keystore certificate for the Administrator tool, you must use a custom keystore certificate for the Content Management Service.

4. Click **Next**.

Informatica 10.5.2

Content Management Service - Step 9D of 12

Enter reference data warehouse database information for the Content Management Service:

Database type:

Database user ID:

Database user password:

Data access connection string:

☒ Schema Name

Configure the database connection:

☐ Enter the JDBC URL.

Database address:

Database service name:

☒ JDBC parameters:

☒ Enter the JDBC connection string.

< Previous Next > Cancel

5. On the **Content Management Service** page, enter the database and user account information for the reference data warehouse database.

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the reference data warehouse. Select one of the following databases. <ul style="list-style-type: none"> <li>- Oracle</li> <li>- IBM DB2</li> <li>- Microsoft SQL Server</li> <li>- Microsoft Azure SQL Database</li> <li>- PostgreSQL, using JDBC</li> </ul>
Database user ID	User account for the reference data warehouse database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

6. Enter the database connection information.

You can specify the connection properties for the JDBC URL or provide the JDBC connection string.

- To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

Property	Description
Database address	Host name and port number for the database in the format <host name>:<port number>.
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

7. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.

8. Click **Next**.

## Profiling Warehouse Connection Database

After you configure the Content Management Service, you can you can configure the data profiling warehouse database.

1. Select the database type for the data profiling warehouse.

The following table lists the databases for the data profiling warehouse.

Prompt	Description
Database type	Type of database for the data profiling warehouse. Select from the following options: <ul style="list-style-type: none"><li>- Oracle</li><li>- Microsoft SQL Server</li><li>- IBM DB2</li></ul>

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the data profiling warehouse user account.
Database user password	Password for the data profiling warehouse user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

3. To specify the schema name, press **1**. If you do not want to specify a schema name, press **2**. Default is 2. If you select Microsoft SQL Server, specify the schema for the repository tables and database connection. If you do not specify a schema name, the installer creates the tables in the default schema.
4. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.
  - a. Enter the JDBC connection information.
    - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	Service or database name : <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li></ul>
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

#### **IBM DB2**

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### **Oracle**

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### **Microsoft SQL Server**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### **Microsoft Azure SQL**

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### **PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### **Azure PostgreSQL**

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

5. Enter the data access connection string.

# PowerCenter Repository Service and the PowerCenter Integration Service

You can configure the PowerCenter Repository Service and the PowerCenter Integration Service.

- 1. If you selected to create a PowerCenter Repository Service and a PowerCenter Integration Service during the installation, the **PowerCenter Repository Service and PowerCenter Integration Service** page appears.

Informatica 10.5

PowerCenter Repository Service and the PowerCenter Integration Service - Step 11 of 12

Enter the required information to configure the PowerCenter Repository Service and the PowerCenter Integration Service.

Database type: Oracle

Database user ID: [redacted]

Database user password: [masked]

Database service name for PowerCenter: RAC19C

PowerCenter Repository Service name: PCRS

PowerCenter Integration Service name: IS

Select PowerCenter Repository Service code page: 7-bit ASCII

Select PowerCenter Integration Service code page: 7-bit ASCII

Next > Cancel

- 2. Select the database to configure for the PowerCenter repository.  
The following table lists the databases you can configure for the PowerCenter repository:

Prompt	Description
Database type	Type of database for the PowerCenter repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - PostgreSQL 4 - IBM DB2 5 - Sybase ASE

- 3. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the PowerCenter repository database user account.
User password	Password for the PowerCenter database user account.
Database service name	Service or database name for PowerCenter: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- PostgreSQL: Enter the database name.</li><li>- IBM DB2: Enter the database name.</li><li>- Sybase ASE: Enter the database name.</li></ul>
Database host name	Enter the PowerCenter repository database.

4. Enter the name of the PowerCenter Repository Service to create.
5. Enter the name of the PowerCenter Integration Service to create.
6. Select the PowerCenter Repository Service code page. Default is 7-bit ASCII.
7. Select the PowerCenter Integration Service code page. Default is 7-bit ASCII.
8. Click **Next**.
9. Click **Done** to close the installer.

The installer creates the PowerCenter Repository Service and PowerCenter Integration Service and starts the services.

The **Post-Installation Summary** page indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## Join a Domain

You can join a domain if you are installing on multiple machines and you have created a domain on another machine.

## Run the Installer

Perform the following steps to run the installer:

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Go to the root of the directory for the installation files and run install.bat as administrator.

To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

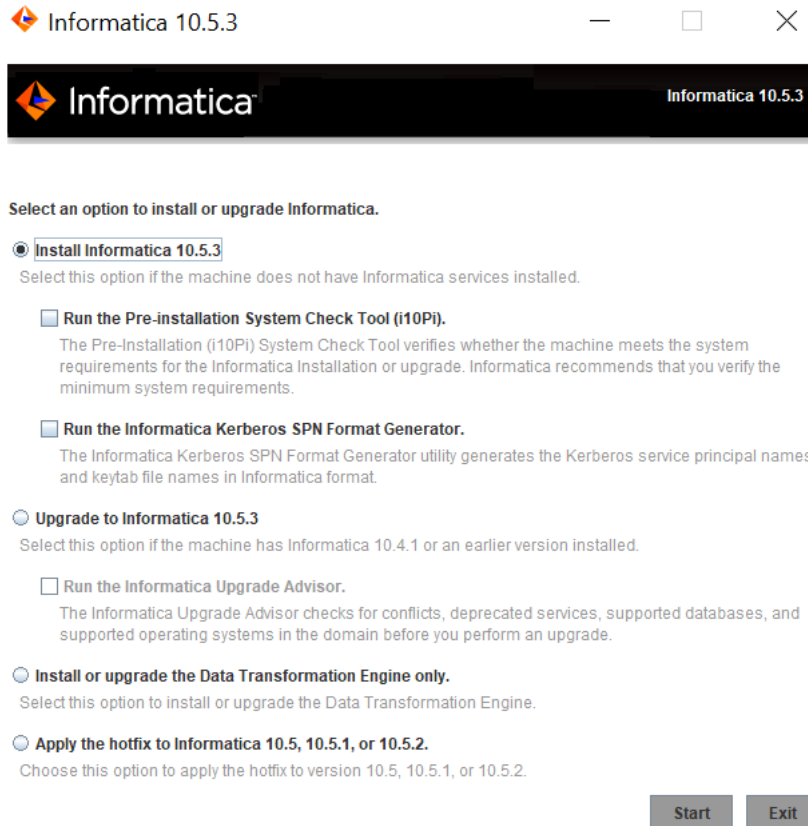
**Note:** If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

The Informatica 10.5.3 page appears.



# Welcome to the Informatica Installer

1. Select **Install Informatica 10.5.3**.



Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

- Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

For more information about running the Pre-Installation (i10Pi) System Check Tool, see [“Run the Pre-Installation \(i10Pi\) System Check Tool in Graphical Mode” on page 105](#).

- Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

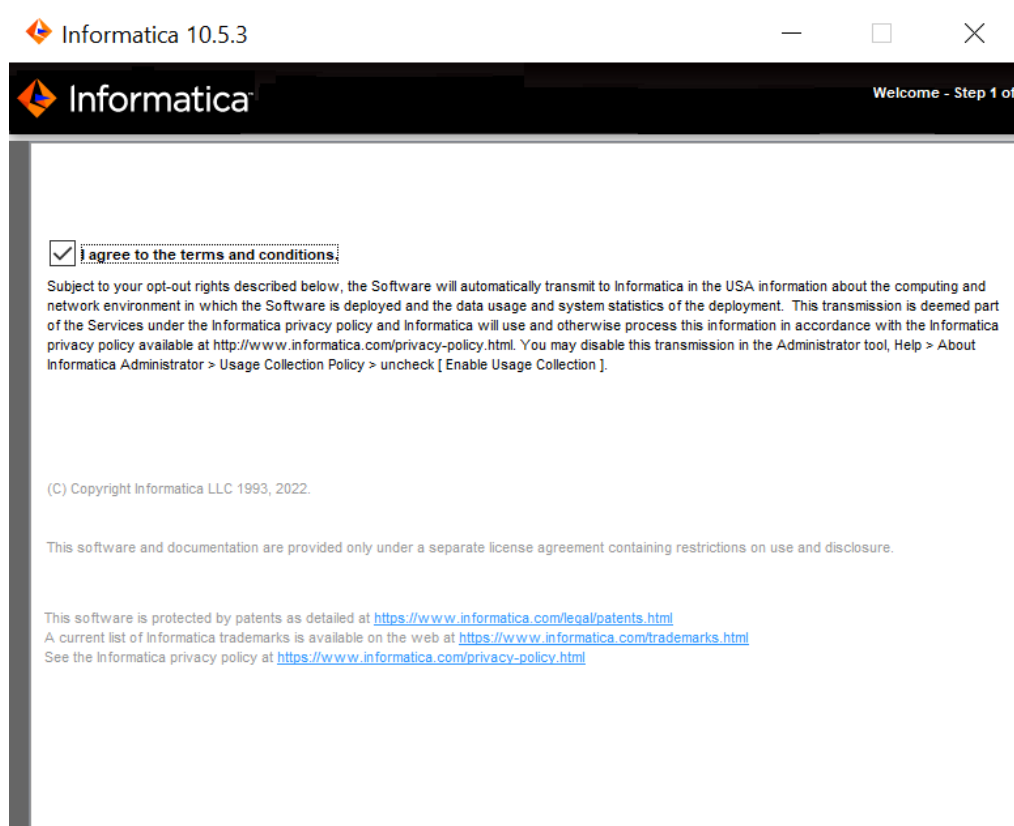
You can use the installer to run the utilities before you install informatica services. After you finish running a utility, restart the installer to run the next utility or install informatica services.

2. Click **Start**.

The **Welcome** section appears.

## Welcome - Accept Terms and Conditions

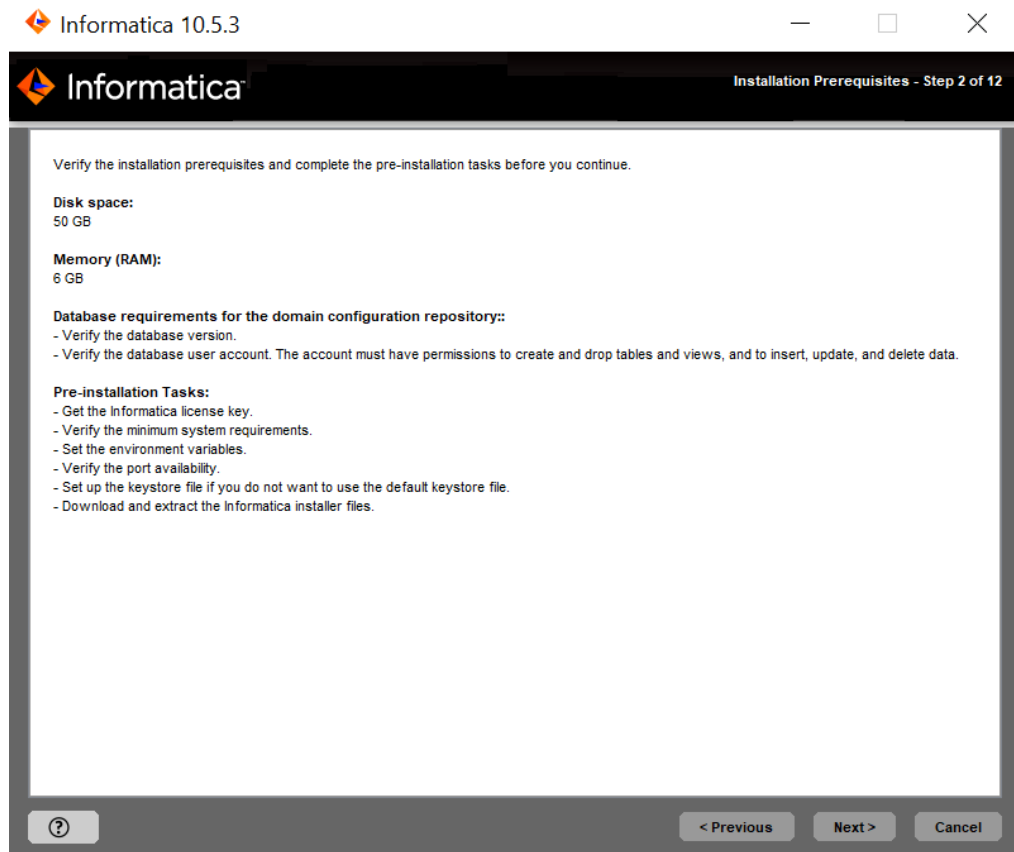
1. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.



Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

2. Click **Next**.

The **Installation Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.



3. Click Next.

The **License and Installation Directory** section appears.

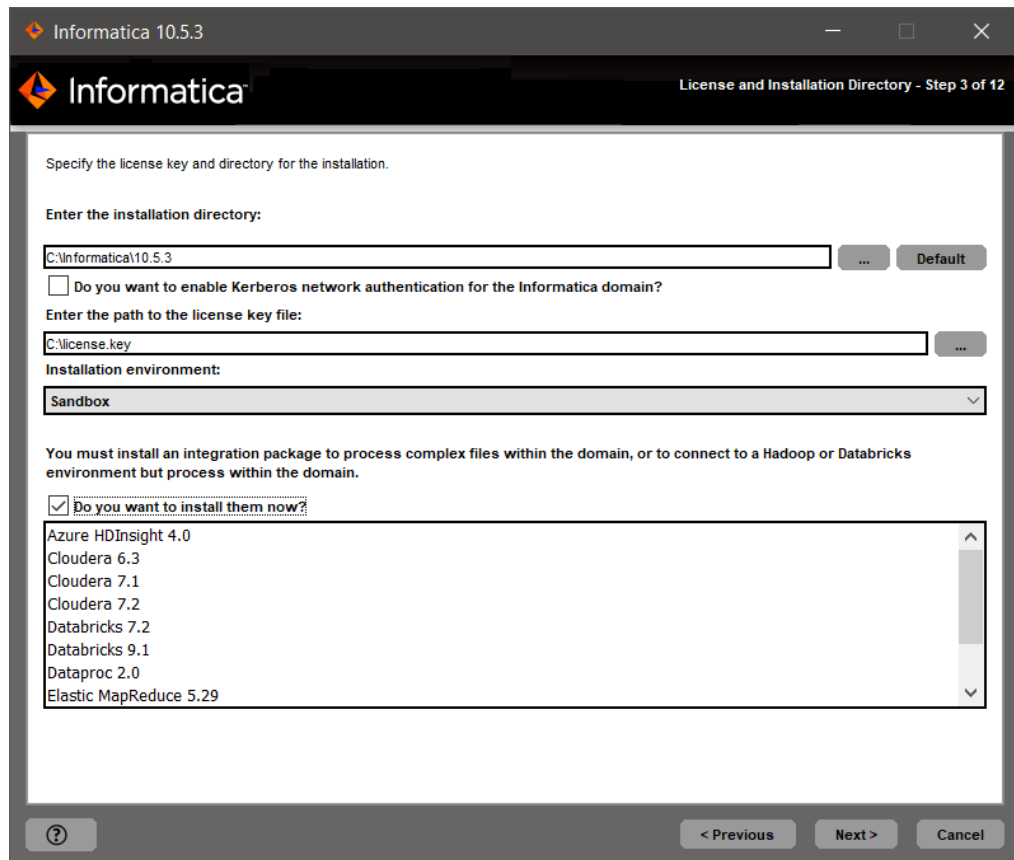
## License and Installation Directory

After you verify the installation prerequisites, you can specify the installation directory.

1. On the **License and Installation Directory** page, enter the Informatica license key, installation directory, installation environment, and distribution packages.

The following table describes the license key, directory that you specify for the Informatica services installation, and the distribution packages installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	<p>Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: @   * \$ # ! % ( ) { } [ ]</p> <p><b>Note:</b> Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.</p>
Installation environment	<p>Environment type associated with the Informatica services installation.</p> <ul style="list-style-type: none"> <li>- Set Sandbox environment for a basic environment used for proof of concept with minimal users.</li> <li>- Set Development environment for the design environment.</li> <li>- Set Test environment for high volume processing that is closest to a production environment.</li> <li>- Set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.</li> </ul>
Distribution packages	<p>You can choose whether to install distribution packages through the Informatica installer.</p> <p>If you choose to install distribution packages, select one or more packages from the list that you want to install.</p>



Informatica 10.5.3

Informatica License and Installation Directory - Step 3 of 12

Specify the license key and directory for the installation.

Enter the installation directory:

C:\Informatica\10.5.3 ... Default

☐ Do you want to enable Kerberos network authentication for the Informatica domain?

Enter the path to the license key file:

C:\license.key ...

Installation environment:

Sandbox

You must install an integration package to process complex files within the domain, or to connect to a Hadoop or Databricks environment but process within the domain.

☒ Do you want to install them now?

- Azure HDInsight 4.0
- Cloudera 6.3
- Cloudera 7.1
- Cloudera 7.2
- Databricks 7.2
- Databricks 9.1
- Dataproc 2.0
- Elastic MapReduce 5.29

? < Previous Next > Cancel

2. Click **Next**.

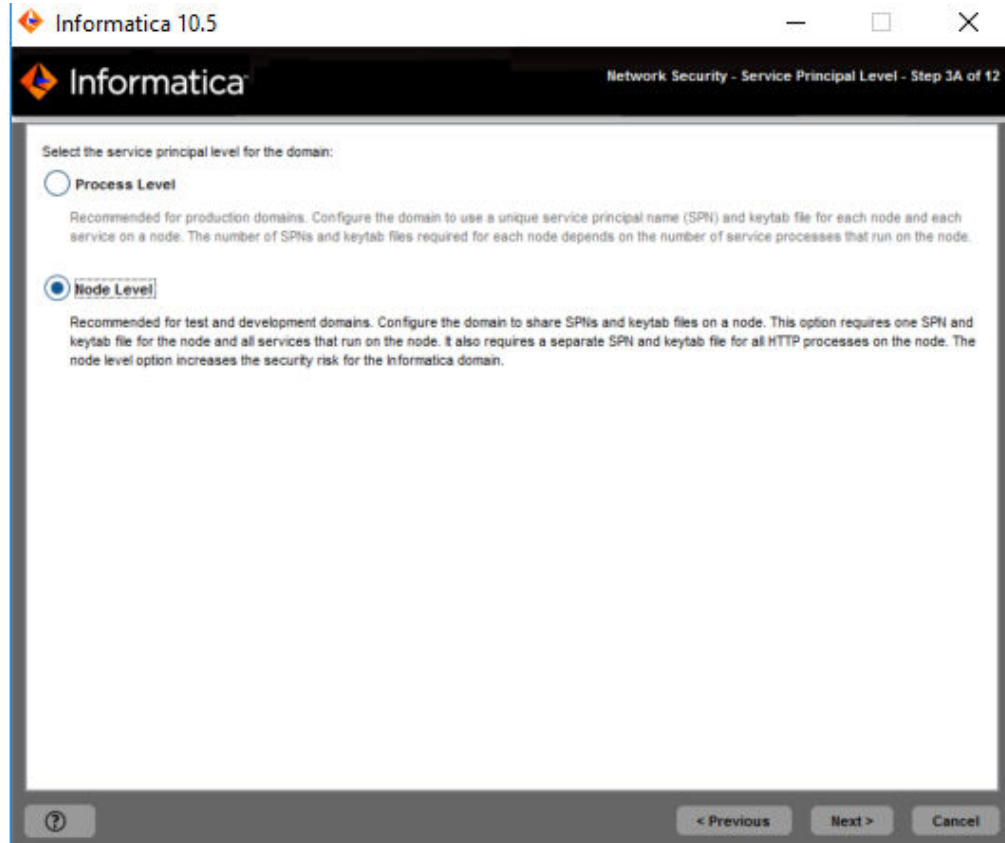
If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“Domain Selection” on page 116](#).

## Network Security - Service Principal Level

After you specify the installation directory, you can configure security level.

1. If you enable Kerberos network authentication, the **Network Security - Service Principal Level** appears.



2. On the **Network Security - Service Principal Level** page, select the level at which to set the Kerberos service principals for the domain.

The following table describes the service principal levels that you can select:

Level	Description
Process Level	<p>Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node.</p> <p>The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.</p>
Node Level	<p>Configures the domain to share SPNs and keytab files on a node.</p> <p>This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node.</p> <p>Use the node level option for domains that do not require a high level of security, such as test and development domains.</p>

3. Click **Next**.

The **Network Security - Kerberos Authentication** section appears.

# Network Security - Kerberos Authentication

After you configure the security level, you can configure Keberos authentication.

1. The **Network Security - Kerberos Authentication** page, enter the domain and keytab information required for Kerberos authentication.

Informatica 10.5.2

Informatica

Network Security - Kerberos Authentication - Step 3B of 12

Specify the Kerberos network authentication parameters.

Domain name:

Installer\_Domain

Node name:

Installer\_Node\_1

Node host name:

informatica.com

Service realm name

COM

User realm name

COM

Keytab directory

E:\keytabs\master

Fully qualified path to the Kerberos configuration file

E:\keytabs\master\krb5.conf

?

< Previous

Next >

Cancel

The following table describes the Informatica domain and node information that you must provide:

Property	Description
Domain name	Name of the domain to create. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the node to create.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. <b>Note:</b> The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	<p>Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive.</p> <p>To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example:</p> <p>*EAST.COMPANY.COM</p>
User realm name	<p>Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive.</p> <p>To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example:</p> <p>*EAST.COMPANY.COM</p>
Keytab directory	<p>Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.</p>
Kerberos configuration file	<p>Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i></p>

**Important:** If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

2. Click **Next**.

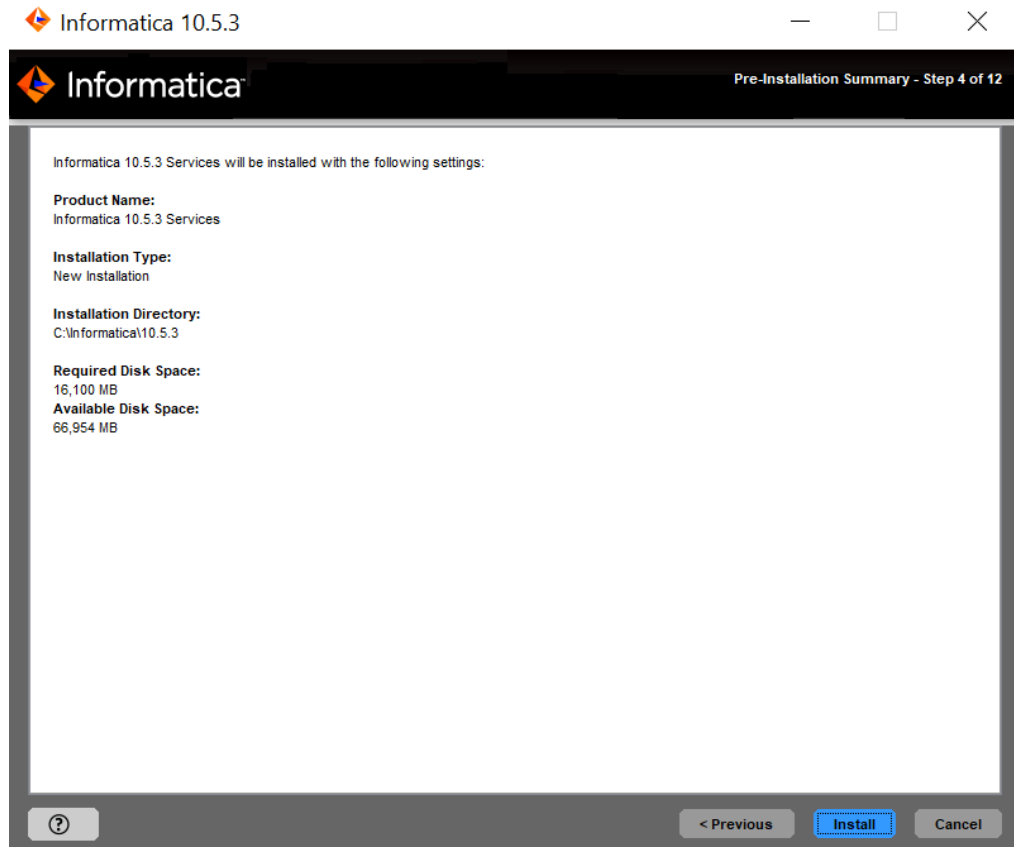
The **Pre-Installation Summary** section appears. Review the installation information.



## Domain Selection

After you review the Pre-Installation summary, you can enter the domain information.

1. Review the **Pre-Installation Summary** page.



2. Review the installation information, and click **Install** to continue.

The installer copies the Informatica files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

Informatica 10.5.2

Domain Selection - Step 5 of 12

Do you want to create a domain or join a domain?

☐ Create a domain.  
Create an Informatica domain if you are installing for the first time or if you are creating multiple domains.

☐ Do you want to enable secure communication for the domain?

☒ Join a domain.  
Join an Informatica domain on another node.

☒ Do you want to join a secure domain?

☐ Do you want this node to be a gateway node?

☒ Enable HTTPS for Informatica Administrator. Port: 8443

☒ Use the default keystore generated by the installer.

☐ Specify the location and password of a custom keystore file.

Keystore password:

Keystore file:

☐ Do you want to enable Security Assertion Markup Language (SAML) authentication?

? Next > Cancel

3. Select **Join a domain**.

The installer joins a node on the machine where you install.

When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.

4. Specify whether the domain you want to join has the secure communication option enabled.

Press **1** to join an unsecure domain or press **2** to join a secure domain.

5. Select the type of node you want to create.

Press **1** to configure a gateway node or **2** to configure a worker node.

If you configure the node as a gateway, you can enable a secure HTTPS connection to the Informatica Administrator.

6. If you enable HTTPS connection for the Informatica Administrator, enter an HTTPS port number to use to secure the connection.

7. Select whether to use the default Informatica SSL certificates or to use your SSL certificates to enable SAML authentication in the domain.

The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

8. To configure Security Assertion Markup Language (SAML) based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, select the checkbox to enable SAML authentication.

**Note:** If you enable Kerberos network authentication, you cannot configure SAML authentication.

9. Click **Next**.

If you select the checkbox to enable SAML authentication option, the **SAML Authentication** page appears.

The screenshot shows the Informatica 10.5.3 SAML Authentication configuration window, titled "SAML Authentication - Step 5A of 12". The window contains the following fields and options:

- Identity Provider URL**
- ☒ Do you want to enter a relying party trust name or a service provider identifier? If you choose No, the service provider identifier will be used.
- Service Provider ID**
- ☒ Enable SAML Assertion Signature Validation
- SAML Assertion Signing Certificate Alias Name**
- Select the truststore for SAML authentication where you imported the identity provider assertion signing certificate:
  - ☒ Use the default Informatica truststore and keystore.
  - ☐ Use a custom truststore and keystore.
- Specify the directory that contains the custom truststore to use for SAML authentication:
- Specify the truststore password
- Specify the directory that contains the custom keystore to use for SAML authentication:
- Specify the keystore password

At the bottom of the window, there is a navigation bar with a help icon (?), "< Previous", "Next >", and "Cancel" buttons.

**Informatica** SAML Authentication - Step 5A of 12

Specify the directory that contains the custom keystore to use for SAML authentication:

Specify the keystore password:

**Authentication Context Comparison**

**Authentication Context Class**

☒ Enable SAML Request Signing Configuration

SAML Request Signing Private Key Alias Name:

SAML Request Signing Private Key Password:

SAML Request Signing Algorithm:

☒ Enable SAML Response Signature Validation

SAML Response Signing Certificate Alias Name:

☒ Enable SAML Assertion Encryption Configuration

Encrypted Assertion Private Key Alias Name:

Encrypted Assertion Private Key Password:

< ? < Previous Next > Cancel

10. Enter the Identity Provider URL for the domain.
11. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you choose No, the service provider identifier is set to "Informatica".
12. Specify whether IdP will sign SAML assertion or not.
13. Enter the identity provider assertion signing certificate alias name.
14. Specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

15. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	Specify the directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

16. To specify the Authentication Context Comparison, specify the strength comparison of the authentication mechanism used by the user with the IdP server.  
Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.
17. To set the Authentication Context Class, specify the expected mechanism of first time authentication of the user with the IdP server.  
Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.
18. Specify if you want to enable the webapp to sign the SAML authentication request or not?  
Default is disabled.
19. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
20. Specify the password to access the private key used for signing the SAML request.
21. Specify the algorithm that the web application uses to sign the SAML request.  
Supported values are RSA\_SHA256, DSA\_SHA1, DSA\_SHA256, RSA\_SHA1, RSA\_SHA224, RSA\_SHA384, RSA\_SHA512, ECDSA\_SHA1, ECDSA\_SHA224, ECDSA\_SHA256, ECDSA\_SHA384, ECDSA\_SHA512, RIPEMD160, or RSA\_MD5.
22. Specify whether you want IdP to sign the SAML response or not?  
Choose to select to enable the webapp to receive the signed SAML response or not. Default is disabled.
23. Specify whether IdP will encrypt SAML assertion or not.  
Select to enable the webapp to receive an encrypted SAML assertion. Default is enabled.
24. Specify the alias name of the private key present in the gateway nodes gateway node SAML truststore that used for Informatica uses to decrypt decrypting the SAML assertion.
25. Provide the password to access the private key to use when decrypting the assertion encryption key.
26. Click **Next**.

If you do not enable secure communication for the domain, the **Domain Configuration** page appears. Skip to step that describes the Domain Configuration Repository page. If you selected the checkbox to enable secure communication for the domain, the **Domain Security - Secure Communication** page appears.

## Domain Security - Secure Connection

After you configure the domain, you can configure domain security.

1. On the **Domain Security - Secure Communication** page, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

Informatica 10.5.3

Domain Security - Secure Communication - Step 58 of 12

Select the SSL certificates to enable secure communication within the domain:

☒ Use the default Informatica SSL certificates contained in the default keystore and truststore.

☐ Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the c

Keystore file directory:

Keystore password:

Truststore file directory:

Truststore password:

< >

? < Previous Next > Cancel

The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	<p>Use the default SSL certificates provided by Informatica.</p> <p><b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.</p>
Use custom SSL certificates	<p>Specify the path of the keystore and truststore files that contain the SSL certificates.</p> <p>You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files.</p> <p>Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain.</p> <p>Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.</p> <p>To set the private truststore files, you must manually import the certificates. Run the <code>keytool</code> command in the <code>&lt;INFA_JDK_HOME&gt;</code> directory to import the private truststore certificates. For example, use the following <code>keytool</code> command:</p> <pre>keytool -noprompt -importkeystore -srckeystore &lt;source truststore file path&gt; -srcstorepass &lt;source truststore file password&gt; -srcalias &lt;alias&gt; -srcstoretype JKS -destkeystore &lt;destination truststore file path&gt; -deststorepass &lt;destination truststore file password&gt; -keypass &lt;private key password&gt; -deststoretype JKS</pre>

2. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named <code>infa_keystore.jks</code> and <code>infa_keystore.pem</code> .
Keystore password	Password for the keystore <code>infa_keystore.jks</code> .
Truststore file directory	Directory that contains the truststore files. The directory must contain files named <code>infa_truststore.jks</code> and <code>infa_truststore.pem</code> .
Truststore password	Password for the <code>infa_truststore.jks</code> file.

3. Click **Next**.

The **Domain Configuration** section appears.



## Domain Configuration

After you configure domain security, you can configure domain repository connection details.

- Enter the information for the domain that you want to join.

The following table describes the properties that you specify for the domain:

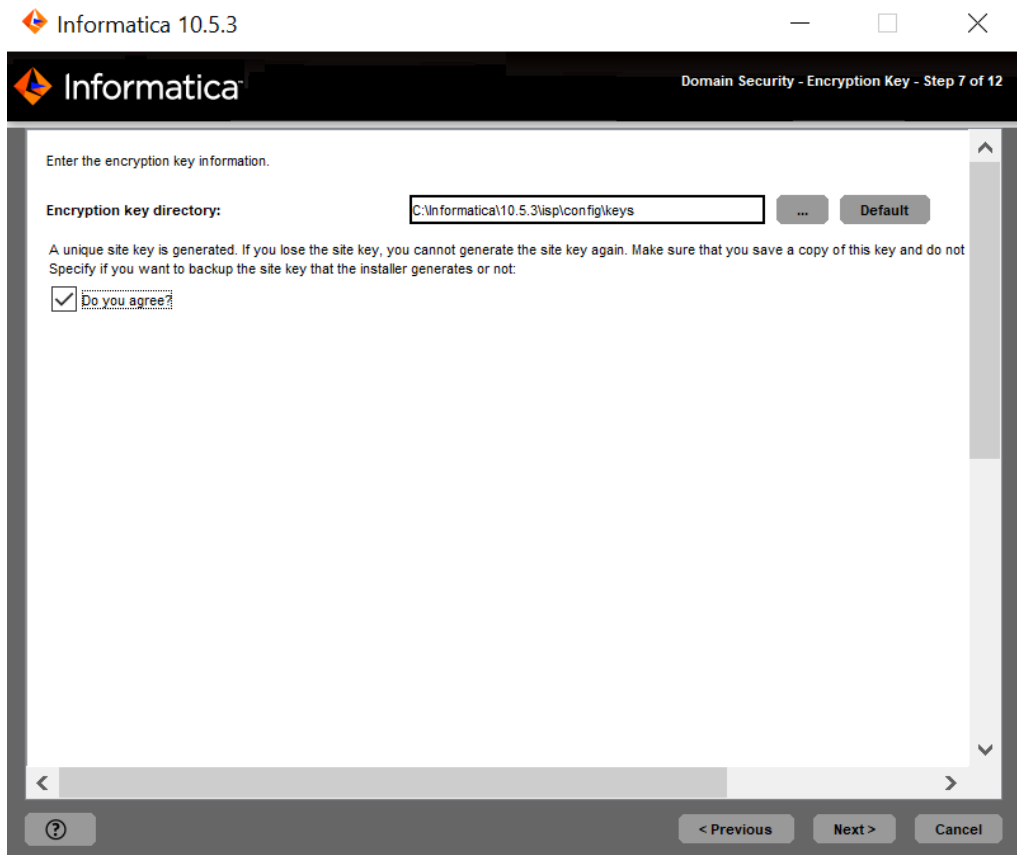
Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.
Gateway node port	Port number of the gateway node.
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.
Security domain name	Name of the secure domain.

The **Domain Security - Encryption Key** section appears.

# Domain Security - Encryption Key

After you configure domain repository, you can configure encryption key.

1. In the **Domain Security - Encryption Key** section, enter the encryption key parameters that you must specify when you create a domain.



The following table describes the encryption key parameters that you must specify when you create a domain:

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: <Informatica installation directory>/isp/config/keys.
Specify if you want to back up the site key that the installer generates or not:	<p>A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.</p> <p>Specify if you want to back up the site key that the installer generates or not:</p> <ul style="list-style-type: none"><li>- Select 1 for No. If you choose No, the installer exits.</li><li>- Select 2 for Yes. If you choose Yes, you agree to back up the file manually.</li></ul>

The installer sets different permissions to the directory and the files in the directory. For more information about the permissions for the encryption key file and directory, see [“Secure Files and Directories” on page 100](#).

2. Click **Next**.

The **Domain and Node Configuration** section appears.

## Join Domain Node Configuration

After you configure the encryption key, you can configure the join domain and node.

1. Enter the information for the domain and the node that you want to join.

The following table describes the properties that you set for the current node.

Property	Description
Node host name	Host name or IP address of the machine on which to join the node. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. <b>Note:</b> The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.
Node name	Name of the node to join.
Node port number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.

2. Select whether to display the advanced port configurations for the domain and node components assigned by the installer.

If you disable the port configurations option, the installer does not display the port configurations. If you enable the port configurations option, the **Port Configuration** section appears. The installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.

3. Select whether you want to create the Model Repository Service and Data Integration Service.

If you choose to create the services, the **Model Repository Service** and the **Data Integration Service** sections appear.

4. Select whether you want to create the PowerCenter Repository Service and the PowerCenter Integration Service.

If you choose to create the services, the **PowerCenter Repository Service and the PowerCenter Integration Service** section appears.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

# Port Configuration

You can update the port numbers for the Service Manager and Informatica Administrator.

1. If you selected to display the port configuration page, the **Port Configuration** page appears.

The screenshot shows the 'Port Configuration - Step 8A of 12' window in Informatica 10.5.2. The window has a title bar with the Informatica logo and version. The main content area is titled 'Enter the port number for the Service Manager.' and contains four input fields: 'Service Manager port' (13242), 'Service Manager shutdown port' (13243), 'Minimum port number' (13250), and 'Maximum port number' (13350). Below these fields is a section titled 'Enter a range of port numbers for service processes in the node.' with two more input fields: 'Minimum port number' (13250) and 'Maximum port number' (13350). At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

2. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

Verify that the port numbers you enter are not used by other applications.  
The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.

Port	Description
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

3. Click **Next**.

The **Windows Service Configuration** page appears.

## Windows Service Configuration

1. If you do not select to display the port configuration page, the installer displays the **Windows Service Configuration** page.

2. On the **Windows Service Configuration** page, select whether to run the Windows service under a different user account.

The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. Click **Next**.

If you do not choose to create the services, the installer displays the **Post-Installation Summary** page. The **Post-Installation Summary** page indicates whether the installation completed successfully.

If you select to configure the Informatica application services, the installer displays the **Model Repository Service Database** page.

## Configure Model Repository Service Database

After you configure the domain and the node, you can configure the Model repository database properties.

1. On the **Model Repository Service Database** page, enter the database and user account information for the Model repository.

Model Repository Service name:

Enter database information for the Model repository:

Database type:

Database user ID:

Database user password:

☐ Is the database secure?

Database connection

( ) Enter the JDBC URL.

Database address:

Database service name:

☒ JDBC parameters:

(●) Enter the JDBC connection string.

<

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: <ul style="list-style-type: none"> <li>- Oracle</li> <li>- IBM DB2</li> <li>- Microsoft SQL Server</li> <li>- PostgreSQL</li> </ul>
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enable secure communication for the domain, you can create the Model repository in a database secured with the SSL protocol. To create a secure Model repository, skip to step [3](#).

2. Enter the database connection information.

If you do not create a secure Model repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

- To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format <code>host_name:port</code> .
Database service name	Service or database name: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- IBM DB2: Enter the service name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.



- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

#### IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

#### Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

#### Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

#### Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

#### Azure SQL Database with Active Directory authentication

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

#### PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

#### Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

Verify that the connection string contains all the connection parameters required by your database system.

3. Choose whether to create a secure Model repository.

If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

For information about the security parameters you must include in the JDBC connection for a secure database, see [“Connection String to a Secure Database” on page 96](#).

4. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
5. Click **Next**.

The **Service Parameters** section appears.

# Data Integration Service

After you configure the Model Repository database, you can configure the service parameters for the application services.

1. On the **Data Integration Service** page, configure the Data Integration Service properties.

Informatica 10.5.3

Informatica Data Integration Service - Step 9C of 12

Enter a name for the Data Integration Service.

Data Integration Service name: DIS

Enter the security properties:

Enter protocol for the Data Integration Service: https

HTTPS port:

☒ Select the SSL certificates to secure the Data Integration Service:

☒ Use the default Informatica SSL certificates contained in the default keystore and truststore.

☐ Enter the location of the SSL certificate files.

Keystore file: C:\Informatica\10.5.3\services\shared\security\infa\_keystore.jks

Keystore password: .....

Truststore file: C:\Informatica\10.5.3\services\shared\security\infa\_truststore.jks

Truststore password: .....

Next > Cancel

The following table describes services parameters that you must set:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: <ul style="list-style-type: none"><li>- HTTP. Requests to the service uses an HTTP connection.</li><li>- HTTPS. Requests to the service uses a secure HTTP connection.</li><li>- HTTP&amp;HTTPS. Requests to the service can use either an HTTP or HTTPS connection.</li></ul>
HTTP port	Port number to used for the Data Integration Service. Default is 6030.

2. If you select an HTTPS connection, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure the connection to the Data Integration Service.

The following table describes the SSL certificate options for securing the Data Integration Service:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. <b>Note:</b> If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Enter the location of the SSL certificate files	Specify the path of the keystore and truststore files that contain the SSL certificates.

If you provide the certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name of the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.
Truststore file	Required. Path and file name of the truststore file that contains the public key for the database.
Truststore password	Required. Password for the truststore file for the secure database.

3. Click **Next**.

The installer creates the Data Integration Service.

# PowerCenter Repository Service and the PowerCenter Integration Service

You can configure the PowerCenter Repository Service and the PowerCenter Integration Service.

- 1. If you selected to create a PowerCenter Repository Service and a PowerCenter Integration Service during the installation, the **PowerCenter Repository Service and PowerCenter Integration Service** page appears.

Informatica 10.5

PowerCenter Repository Service and the PowerCenter Integration Service - Step 11 of 12

Enter the required information to configure the PowerCenter Repository Service and the PowerCenter Integration Service.

Database type: Oracle

Database user ID: [Redacted]

Database user password: [Masked]

Database service name for PowerCenter: RAC19C

PowerCenter Repository Service name: PCRS

PowerCenter Integration Service name: IS

Select PowerCenter Repository Service code page: 7-bit ASCII

Select PowerCenter Integration Service code page: 7-bit ASCII

Next > Cancel

- 2. Select the database to configure for the PowerCenter repository.
- The following table lists the databases you can configure for the PowerCenter repository:

Prompt	Description
Database type	Type of database for the PowerCenter repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - PostgreSQL

- 3. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the PowerCenter repository database user account.
User password	Password for the PowerCenter database user account.
Database service name	Service or database name for PowerCenter: <ul style="list-style-type: none"><li>- Oracle: Enter the service name.</li><li>- Microsoft SQL Server: Enter the database name.</li><li>- PostgreSQL: Enter the database name.</li></ul>
Database host name	Enter the PowerCenter repository database.

4. Enter the name of the PowerCenter Repository Service to create.
5. Enter the name of the PowerCenter Integration Service to create.
6. Select the PowerCenter Repository Service code page. Default is 7-bit ASCII.
7. Select the PowerCenter Integration Service code page. Default is 7-bit ASCII.
8. Click **Next**.
9. Click **Done** to close the installer.

The installer creates the PowerCenter Repository Service and PowerCenter Integration Service and starts the services.

The **Post-Installation Summary** page indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

## CHAPTER 10

# Run the Silent Installer

This chapter includes the following topics:

- [Installing in Silent Mode, 231](#)
- [Encrypting Passwords in the Properties File, 232](#)

## Installing in Silent Mode

To install without user interaction, install in silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the services on multiple machines on the network or to standardize the installation across machines.

Copy the installation files to the hard disk on the machine where you plan to install the services. If you install on a remote machine, verify that you can access and create files on the remote machine.

To install in silent mode, complete the following tasks:

1. Run the password encryption utility to encrypt the passwords in the installation properties file.
2. Configure the installation properties file and specify the installation options in the properties file.
3. Run the installer with the installation properties file.

## Configure the Properties File

Configure the properties file that contains the configuration properties required to install the Informatica services in silent mode.

Informatica provides two versions of the properties file. Use either file to specify the options for your installation.

### **Silent input properties file**

The silent input properties file contains the configuration properties required to install the Informatica services in silent mode. Use the file if you want to consider the appropriate value to set for each property in the file.

### **Default silent input properties file**

The default silent input properties file contains default values for many configuration properties. The properties are listed in the bottom portion of the file. Use the file if you plan to install the Informatica services using the default property values.

The file contains properties set to the default value for the following options:

- Application service names.
- Secure Sockets Layer authentication.
- Kerberos authentication.
- Port number assignment for domain and node components.

To configure the properties file that contains the configuration properties required to install the Informatica services in silent mode, complete the following steps:

1. Go to the root of the directory that contains the installation files.
2. Optionally, run the password encryption utility to encrypt passwords in the .properties file.
3. Create a backup copy of the `SilentInput.properties` file.
4. Open either the `SilentInput.properties` file or the `SilentInput_Default.properties` file.
5. Configure the properties in the file.
6. Save the file with the name `SilentInput.properties`.

## Run the Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file `SilentInput.properties` that you edited and resaved.
4. Run the silent installation. On Linux, run `silentInstall.sh`.

The silent installer runs in the background. The process can take a while. The silent installation is complete when the `Informatica_<Version>_Services_InstallLog<timestamp>.log` file is created in the installation directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

## Encrypting Passwords in the Properties File

The installer includes a utility that you can use to encrypt passwords you set in the properties file you use to specify options when you run the installer in silent mode. Informatica uses AES encryption with multiple 256-bit keys to encrypt passwords.

You run the utility for each password you want to encrypt. When you run the utility, you specify the value of the password in plain text at the command prompt. The utility generates the password in encrypted format as output. The output includes the following prefix: `=INSTALLER:CIPHER:AES:256=`

Copy the complete output string, including the prefix, and then paste it into the properties file as the value for the password property. When you run the installer in silent mode, the installation framework decrypts the password.

1. Go to the utility directory:  

```
<Installer directory>/properties/Utils/passwd_encryption
```



2. Run the utility. Specify the plain text password you want to encrypt as the value for <password>.

- On Linux and UNIX, run the following command:

```
sh install.sh <password>
```

- On Windows, run the following command:

```
install.bat <password>
```

3. Copy the encrypted password string from the output, and then paste the string into the .properties file as the value for the corresponding password.

The following example shows the encrypted password set as the value for the DOMAIN\_PSSWD property:

```
DOMAIN_PSSWD==INSTALLER:CIPHER:AES:256=mjkjmDR2kzFJiizfRWIOPg==
```

# CHAPTER 11

## Troubleshooting

This chapter includes the following topics:

- [Installation Troubleshooting Overview, 234](#)
- [Resuming a Failed Installer Process, 234](#)
- [Troubleshooting with Installation Log Files, 235](#)
- [Troubleshooting Domains and Nodes, 237](#)
- [Troubleshooting Informatica Developer, 239](#)

### Installation Troubleshooting Overview

The topics in this section provides you information on troubleshooting probable issues that you might encounter during Informatica installation process. The examples included in the topics describe general troubleshooting strategies and are not a comprehensive list of possible causes of installation issues.

### Resuming a Failed Installer Process

When the installation process stops midway, you can resume the installation from the point of failure or exit.

When the service installation process fails on UNIX or Linux, you can resume from the previous service configuration and recover the last entered details for that service installation. The install process might fail for reasons such as network outage, when you exit the installation before completing the entire installation process, or because of incorrect information entered.

Consider the following guidelines for resuming the installation:

**You can resume the installer**

If a service fails or if the installation process fails during a service creation, you can resume the installation process with the server installer. To resume the installation process, ensure that at least one of the services is created and that the domain is up and running from the installation log. For example, if you want to check whether the Model Repository Service is created, check if you have a service creation success text in the server log in the following format:

```
SUCCESS: MRS Service [mrs_name] is created. Command ran successfully.
```

To resume the installation, run the installer again.

When you resume the installer while creating a service, the installer retains all the service and database specific information, such as the create service status, service name, service enabled or disabled status. You can confirm and use the previously entered values or specify new values for the service and resume the installation process.

#### **You cannot resume the installer**

You cannot resume the installer in the following situations:

- You run installer to configure services after the services are created.
- You run the service configuration wizard.
- You join a domain.

## Before You Resume the Installer

When the installation process stops midway, you can resume the installation from the point of failure or exit.

Before you can resume the installer, complete the following prerequisites:

1. In the installation log file present in the installation directory, verify that at least the domain and one service is created. The installer log file name appears in the following syntax:  
Informatica\_<Version>\_Services\_<timestamp>.log
2. Ensure that you do not delete the installInst.obj object file present in the tools folder of the user installation directory.
3. If you are going to resume through the silent installer, ensure that RESUME\_INSTALLATION is set to true in the SilentInput.properties file.

## Resume the Installer

After you complete prerequisite tasks, you can resume the installer.

1. Open a command prompt and navigate to the location of the installation files.
2. Run the console installer or the silent installer.
3. When the regular installer runs, you might get a prompt confirming whether you want to resume previous installer or not.
  - If you do not want to resume installation, enter 1 for No. Default is 1.
  - If you want to resume installation, enter 2 for Yes.

Before you can resume the installation, the services get validated.

# Troubleshooting with Installation Log Files

You can use the following log files to troubleshoot an Informatica installation:

#### **Installation log files**

The installer produces log files during and after the installation. You can use these logs to get more information about the tasks completed by the installer and errors that occurred during installation. The installation log files include the following logs:

- Debug logs

- File installation logs

#### Service Manager log files

Log files generated when the Service Manager starts on a node.

## Debug Log Files

The installer writes actions and errors to the debug log file. The name of the log file depends on the Informatica component you install.

The debug log contains output from the infacmd and infasetup commands used to create the domain, node, and application services. It also contains information about starting the application services.

The following table describes the properties of the debug log files:

Property	Description
Log File Name	<ul style="list-style-type: none"> <li>- Informatica_&lt;Version&gt;_Services_&lt;timestamp&gt;.log</li> <li>- Informatica_&lt;Version&gt;_Client_&lt;timestamp&gt;.log</li> <li>- Informatica_&lt;Version&gt;_Services_Upgrade_&lt;timestamp&gt;.log</li> <li>- Informatica_&lt;Version&gt;_Client_Upgrade_&lt;timestamp&gt;.log</li> </ul>
Location	Installation directory.
Usage	Get more information about the actions performed by the installer and get more information about installation errors. The installer writes information to this file during the installation. If the installer generates an error, you can use this log to troubleshoot the error.
Contents	Detailed summary of each action performed by the installer, the information you entered in the installer, each command line command used by the installer, and the error code returned by the command.

## File Installation Log File

The file installation log file contains information about the installed files.

The following table describes the properties of the installation log file:

Property	Description
Log File Name	<ul style="list-style-type: none"> <li>- Informatica_&lt;Version&gt;_Services_InstallLog.log</li> <li>- Informatica_&lt;Version&gt;_Client_InstallLog.log</li> </ul>
Location	Installation directory.
Usage	Get information about the files installed and registry entries created.
Contents	Directories created, names of the files installed and commands run, and status for each installed file.

## Service Manager Log Files

The installer starts the Informatica service. The Informatica service starts the Service Manager for the node. The Service Manager generates log files that indicate the startup status of a node. Use these files to

troubleshoot issues when the Informatica service fails to start and you cannot log in to Informatica Administrator. The Service Manager log files are created on each node.

The following table describes the files generated by the Service Manager:

Property	Description
catalina.out	Log events from the Java Virtual Machine (JVM) that runs the Service Manager. For example, a port is available during installation, but is in use when the Service Manager starts. Use this log to get more information about which port was unavailable during startup of the Service Manager.  The catalina.out file is in the following directory: <Informatica installation directory>/logs/<node name>/catalina.out
node.log	Log events generated during the startup of the Service Manager on a node. You can use this log to get more information about why the Service Manager for a node failed to start. For example, if the Service Manager cannot connect to the domain configuration database after 30 seconds, the Service Manager fails to start. The node.log file is in the /tomcat/logs directory.

**Note:** The Service Manager also uses node.log to record events when the Log Manager is unavailable. For example, if the machine where the Service Manager runs does not have enough available disk space to write log event files, the Log Manager is unavailable.

## Troubleshooting Domains and Nodes

The installer can generate errors when creating and configuring domains and nodes during the Informatica installation.

### Creating the Domain Configuration Repository

If you create a domain, the installer creates a domain configuration repository to store domain metadata. The installer uses the options you enter during installation to add configuration metadata to the domain configuration repository. The installer uses JDBC to communicate with the database. You do not need to configure ODBC or native connectivity on the machine where you install the Informatica services.

The installer creates and drops a table in the domain configuration repository database to verify the connection information. The user account for the database must have create privileges on the database. Each domain must have a separate domain configuration repository.

### Creating or Joining a Domain

The installer completes different tasks depending on whether you create a domain or join a domain:

- **Creating a domain.** The installer runs the `infasetup DefineDomain` command to create the domain and the gateway node for the domain on the current machine based on the information you enter in the Configure Domain window.
- **Joining a domain.** The installer runs the `infasetup DefineWorkerNode` command to create a node on the current machine, and runs the `infacmd AddDomainNode` command to add the node to the domain. The installer uses the information you enter in the Configure Domain window to run the commands.

The `infasetup` and `infacmd` commands fail if the gateway node is unavailable. If the gateway node is unavailable, you cannot log in to Informatica Administrator.

For example, the `DefineDomain` command fails if you click Test Connection and the connection test passes but the database becomes unavailable before you click Next. The `DefineDomain` command can also fail if the host name or IP address does not belong to the current machine. Verify that the database for the domain configuration is available and that the host name is correct and try again.

If the `AddDomainNode` command fails, verify that the Informatica service is running on the gateway node and try again.

## Starting Informatica

The installer runs `infaservice` to start the Informatica service. To troubleshoot issues when Informatica fails to start, use the information in the installation debug log and the `node.log` and `catalina.out` Service Manager log files to identify the cause of the error.

If you create a domain, log in to Informatica Administrator after the Informatica service starts to verify that the domain is available. If you join a domain, log in to Informatica Administrator after the Informatica service starts to verify that the node was successfully created and started.

Informatica can fail to start for the following reasons:

- **The Service Manager is out of system memory.** The Java Runtime Environment (JRE) that starts Informatica and runs the Service Manager may not have enough system memory to start. Set the `INFA_JAVA_OPTS` environment variable to configure the amount of system memory used by Informatica. On UNIX, you can set the memory configuration when you start Informatica.
- **The domain configuration database is not available.** Informatica fails to start on a node if the Service Manager on a gateway node cannot connect to the domain configuration database within 30 seconds. Verify that the domain configuration repository is available.
- **Some of the folders in the Informatica installation directory do not have the appropriate execute permissions.** Grant execute permission on the Informatica installation directory.

## Pinging the Domain

The installer runs the `infacmd Ping` command to verify that the domain is available before it continues the installation. The domain must be available so that license objects can be added to the domain. If the Ping command fails, start Informatica on the gateway node.

## Adding a License

The installer runs the `infacmd AddLicense` command to read the Informatica license key file and create a license object in the domain. To run the application services in Informatica Administrator, a valid license object must exist in the domain.

If you use an incremental license and join a domain, the serial number of the incremental license must match the serial number for an existing license object in the domain. If the serial numbers do not match, the `AddLicense` command fails.

You can get more information about the contents of the license key file used for installation, including serial number, version, expiration date, operating systems, and connectivity options in the installation debug log. You can get more information about existing licenses for the domain in Informatica Administrator.

# Troubleshooting Informatica Developer

Consider the following tips when you work with the Informatica Developer:

## **Informatica Developer fails to launch**

This issue might occur if the jvm.dll of java requires the MSVCR100.dll.

To resolve this issue, download Microsoft Visual C++ Studio 2010 Redistributable Package from the Microsoft website.

# Part IV: After You Install the Services

This part contains the following chapters:

- [Complete the Domain Configuration, 241](#)
- [Prepare to Create the Application Services, 246](#)
- [Create and Configure Application Services, 255](#)



## CHAPTER 12

# Complete the Domain Configuration

This chapter includes the following topics:

- [Checklist to Complete the Domain Configuration, 241](#)
- [Complete the Domain Configuration Overview, 242](#)
- [Verify Locale Settings and Code Page Compatibility, 242](#)
- [Configure Environment Variables on UNIX or Linux, 243](#)

## Checklist to Complete the Domain Configuration

This chapter contains information about domain configuration tasks that you need to complete after installation. Use this checklist to track domain configuration tasks.

- ☐ Verify locale settings and code page compatibility:
  - Verify that the domain configuration database is compatible with the code pages of the application services that you create in the domain.
  - Verify that the locale settings on machines that access the Administrator tool and the Informatica client tools is compatible with the code pages of repositories in the domain.
  - Configure the locale environment variables.
- ☐ Configure the following environment variables:
  - Informatica environment variables to store memory, domain, and location settings.
  - Library path environment variables on the machines that run the Data Integration Service.
  - Kerberos environment variables if you configure the Informatica domain to run on a network with Kerberos authentication.

# Complete the Domain Configuration Overview

After you install Informatica services and before you create the application services, complete the configuration for the domain services.

Domain configuration includes tasks such as verifying code pages, configuring the environment variables for the domain, and configuring the firewall.

## Verify Locale Settings and Code Page Compatibility

The code pages for application services must be compatible with code pages in the domain.

Verify and configure the locale settings and code pages:

**Verify that the domain configuration database is compatible with the code pages of the application services that you create in the domain.**

The Service Manager synchronizes the list of users in the domain with the list of users and group in each application service. If a user name in the domain has characters that the code page of the application service does not recognize, characters do not convert correctly and inconsistencies occur.

**Verify that the locale settings on machines that access the Administrator tool and the Informatica client tools are compatible with code pages of repositories in the domain.**

If the locale setting is not compatible with the repository code page, you cannot create an application service.

## Configure Locale Environment Variables

Verify that the locale setting is compatible with the code page for the repository. If the locale setting is not compatible with the repository code page, you cannot create an application service.

Use LANG, LC\_CTYPE, or LC\_ALL to set the UNIX or Linux code page.

Different operating systems require different values for the same locale. The value for the locale variable is case sensitive.

Use the following command to verify that the value for the locale environment variable is compatible with the language settings for the machine and the type of code page you want to use for the repository:

```
locale -a
```

The command returns the languages installed on the operating system and the existing locale settings.

Set the following locale environment variables:

### Locale on Linux

All UNIX operating systems except Linux have a unique value for each locale. Linux allows different values to represent the same locale. For example, "utf8," "UTF-8," "UTF8," and "utf-8" represent the same locale on a Linux machine. Informatica requires that you use a specific value for each locale on a Linux machine. Make sure that you set the LANG environment variable appropriately for all Linux machines.

### Locale for Oracle database clients

For Oracle database clients, set NLS\_LANG to the locale that you want the database client and server to use with the login. A locale setting consists of the language, territory, and character set. The value of NLS\_LANG depends on the configuration.

For example, if the value is `american_america.UTF8`, set the variable in a C shell with the following command:

```
setenv NLS_LANG american_america.UTF8
```

To read multibyte characters from the database, set the variable with the following command:

```
setenv NLS_LANG=american_america.AL32UTF8
```

You must set the correct variable on the Data Integration Service machine so that the Data Integration Service can read the Oracle data correctly.

## Configure Environment Variables on UNIX or Linux

Informatica uses environment variables to store configuration information when it runs the application services and connects to the clients. Configure the environment variables to meet the Informatica requirements.

Incorrectly configured environment variables can cause the Informatica domain or nodes to fail to start or can cause connection problems between the Informatica clients and the domain.

To configure environment variables, log in with the system user account you used to install Informatica.

### Configure Informatica Environment Variables

You can configure Informatica environment variables to store memory, domain, and location settings.

Set the following environment variables:

#### INFA\_JAVA\_OPTS

By default, Informatica uses a maximum of 512 MB of system memory.

The following table lists the minimum requirement for the maximum heap size settings, based on the number of users and services in the domain:

Number of Domain Users	Maximum Heap Size (1-5 Services)	Maximum Heap Size (6-10 Services)
1,000 or less	512 MB (default)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

**Note:** The maximum heap size settings in the table are based on the number of application services in the domain.

If the domain has more than 1,000 users, update the maximum heap size based on the number of users in the domain.

You can use the `INFA_JAVA_OPTS` environment variable to configure the amount of system memory used by Informatica. For example, to configure 1 GB of system memory for the Informatica daemon in a C shell, use the following command:

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

Restart the node for the changes to take effect.

#### **INFA\_DOMAINS\_FILE**

The installer creates a `domains.infa` file in the Informatica installation directory. The `domains.infa` file contains the connectivity information for the gateway nodes in a domain, including the domain names, domain host names, and domain host port numbers.

Set the value of the `INFA_DOMAINS_FILE` variable to the path and file name of the `domains.infa` file.

Configure the `INFA_DOMAINS_FILE` variable on the machine where you install the Informatica services.

#### **INFA\_HOME**

Use `INFA_HOME` to designate the Informatica installation directory. If you modify the Informatica directory structure, you need to set the environment variable to the location of the Informatica installation directory or the directory where the installed Informatica files are located.

For example, you use a softlink for any of the Informatica directories. To configure `INFA_HOME` so that any Informatica application or service can locate the other Informatica components it needs to run, set `INFA_HOME` to the location of the Informatica installation directory.

#### **INFA\_TRUSTSTORE**

If you enable secure communication for the domain, set the `INFA_TRUSTSTORE` variable with the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named `infa_truststore.jks` and `infa_truststore.pem`.

You must set the `INFA_TRUSTSTORE` variable if you use the default SSL certificate provided by Informatica or a certificate that you provide.

#### **INFA\_TRUSTSTORE\_PASSWORD**

If you enable secure communication for the domain and you specify the SSL certificate to use, set the `INFA_TRUSTSTORE_PASSWORD` variable with the password for the `infa_truststore.jks` that contains the SSL certificate. The password must be encrypted. Use the command line program `pmpasswd` to encrypt the password.

## Configure Library Path Environment Variables

Configure library path environment variables on the machines that run the Data Integration Service processes. The variable name and requirements depend on the platform and database.

Configure the `LD_LIBRARY_PATH` environment variable.

The following table describes the values that you set for the `LD_LIBRARY_PATH` for the different databases:

Database	Value
Oracle	<Database path>/lib
IBM DB2	<Database path>/lib
Sybase ASE	"\${SYBASE_OCS}/lib:\${SYBASE_ASE}/lib:\${LD_LIBRARY_PATH}"

Database	Value
Informix	<Database path>/lib
Teradata	<Database path>/lib
ODBC	<CLOSEDODBCHOME>/lib
PostgreSQL	\$PGHOME/lib:\$ {LD_LIBRARY_PATH}

## Configure Kerberos Environment Variables

If you configure the Informatica domain to run on a network with Kerberos authentication, you must set the Kerberos configuration and credential cache environment variables.

Set the following environment variables:

### KRB5\_CONFIG

Use the KRB5\_CONFIG environment variable to store the path and file name of the Kerberos configuration file. The name of the Kerberos configuration file is *krb5.conf*. You must set the KRB5\_CONFIG environment variable on each node in the Informatica domain.

### KRB5CCNAME

Set the KRB5CCNAME environment variable with the path and file name of the Kerberos user credential cache. Kerberos single sign-on requires Kerberos credential cache for user accounts.

When you cache the user credential, you must use the *forwardable* option. For example, if you use *kinit* to get and cache the user credential, you must use the *-f* option to request forwardable tickets.

## CHAPTER 13

# Prepare to Create the Application Services

This chapter includes the following topics:

- [Checklist for Preparing to Create Application Services, 246](#)
- [Create Directories for the Analyst Service, 247](#)
- [Create a Keystore for a Secure Connection to a Web Application Service, 247](#)
- [Log In to Informatica Administrator, 248](#)
- [Create Connections, 249](#)

## Checklist for Preparing to Create Application Services

This chapter contains tasks that you need to complete before you create or configure the Analyst Service, the Data Integration Service, and the Content Management Service. When you configure the services you configure properties based on the connections and directories that you create. Use this checklist to track the configuration tasks.

- ☐ Create the following directories for the Analyst Service:
  - Flat file caches
  - Temporary business glossary files
  - Glossary assets
- ☐ Create the following connections for the Data Integration Service:
  - Data object cache database
  - Workflow database
  - Profiling warehouse
- ☐ Create the following connection for the Content Management Service:
  - Reference data warehouse

# Create Directories for the Analyst Service

Before you create the Analyst Service, you must create directories for the Analyst tool to store temporary files.

Create the following directories on the node that runs the Analyst Service:

## **Flat file cache directory**

Create a directory for the flat file cache where the Analyst tool stores uploaded flat files. The Data Integration Service must also be able to access this directory. If the Analyst Service and the Data Integration Service run on different nodes, configure the flat file directory to use a shared directory. If the Data Integration Service runs on primary and back-up nodes or on a grid, each Data Integration Service process must be able to access the files in the shared directory.

For example, you can create a directory named "flatfilecache" in the following mapped drive that all Analyst Service and Data Integration Service processes can access:

```
F:\shared\<Informatica installation directory>\server
```

When you import a reference table or flat file source, the Analyst tool uses the files from this directory to create a reference table or flat file data object.

## **Temporary export file directory**

Create a directory to store the temporary business glossary files that the business glossary export process creates. Create the directory on the node that runs the Analyst Service.

For example, you can create a directory named "exportfiledirectory" in the following location:

```
<Informatica installation directory>/server
```

## **Asset attachments directory**

Create a directory to store the files that content managers add as attachments to Glossary assets. Create the directory on the node that runs the Analyst Service.

For example, you can create a directory named "attachmentdirectory" in the following location:

```
<Informatica installation directory>/server
```

# Create a Keystore for a Secure Connection to a Web Application Service

You can secure the connection between the Informatica domain and a web application service, such as the Analyst service. Informatica uses the SSL/TLS protocol to encrypt network traffic. To secure the connection, you must create the required files.

Before you can secure the connection to a web application service, verify that the following requirements are met:

## **You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

## **You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

**The keystore is in an accessible directory.**

The keystore must be in a directory that is accessible to the Administrator tool.

## Log In to Informatica Administrator

You must have a user account to log in to the Informatica Administrator web application.

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer, Microsoft Edge, and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. In Safari, add the certificate of the Informatica web application to the keychain. If you are using Chrome version 86.0.42x or later on Windows, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:
  - If the Administrator tool is not configured to use a secure connection, enter the following URL:  
`http://<fully qualified hostname>:<http port>/administrator/`
  - If the Administrator tool is configured to use a secure connection, enter the following URL:  
`https://<fully qualified hostname>:<https port>/administrator/`

Host name and port in the URL represent the host name and port number of the master gateway node. If you configured secure communication for the domain, you must use HTTPS in the URL to ensure that you can access the Administrator tool.

If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

3. If you do not use Kerberos authentication, enter the user name, password, and security domain for your user account, and then click **Login**.

The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. If you do not know the security domain that your user account belongs to, contact the Informatica domain administrator.

**Note:** If this is the first time you log in with the user name and password provided by the domain administrator, change your password to maintain security.

## Troubleshooting the Login to Informatica Administrator

If the Informatica domain uses Kerberos authentication, you might encounter the following issues when logging in to the Administrator tool:



**I cannot log in to the Administrator tool from the same machine where I created the domain gateway node.**

After installation, if you cannot log in to the Administrator tool from the same machine where you created the domain gateway node, clear the browser cache. When you initially log in to the Administrator tool after installation, you can only log in with the Administrator user account created during installation. If a different user credential is stored in the browser cache, the login can fail.

**A blank page appears after I log in to the Administrator tool.**

If a blank page appears after you log in to the Administrator tool, verify that you enabled delegation for all user accounts with service principals used in the Informatica domain. To enable delegation, in the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

## Create Connections

In the Administrator tool, create connections to the databases that the application services use. You need to specify the connection details while you configure the application service.

When you create the database connection, specify the database connection properties and test the connection.

The following table describes the database connections that you need to create before the application services can access the associated databases.

Database Connection	Description
Data object cache database	To access the data object cache, create the data object cache connection for the Data Integration Service.
Workflow database	To store run-time metadata for workflows, create the workflow database connection for the Data Integration Service.
Profiling warehouse database	<p>To create and run profiles and scorecards, create the profiling warehouse database connection for the Data Integration Service.</p> <p>Use this instance of the Data Integration Service when you configure the run-time properties of the Analyst Service.</p> <p><b>Note:</b> To use the Microsoft SQL Server database as the profiling warehouse, choose ODBC as the provider type, and clear the <b>use DSN</b> option in the <b>Microsoft SQL Server connection properties</b> dialog box when you configure the Microsoft SQL Server connection.</p>
Reference data warehouse	To store reference table data, create the reference data warehouse connection for the Content Management Service.

## IBM DB2 Connection Properties

Use a DB2 for LUW connection to access tables in a DB2 for LUW database.

The following table describes the DB2 for LUW connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
Connection String for metadata access	Connection string to import physical data objects. Use the following connection string: <code>jdbc:informatica:db2://&lt;host&gt;:50000;databaseName=&lt;dbname&gt;</code>
Connection String for data access	Connection string to preview data and run mappings. Enter <code>dbname</code> from the alias configured in the DB2 client.
Code Page	Database code page.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Tablespace	Tablespace name of the DB2 for LUW database.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

## Microsoft Azure SQL Database Connection Properties

Use an Azure SQL Data Warehouse connection to access tables in a Microsoft Azure SQL database.

The following table describes the Microsoft Azure SQL Database connection properties:

Property	Description
Azure DW JDBC URL	Connection string to the Microsoft Azure SQL database.
Azure DW JDBC Username	Database user name.

Property	Description
Azure DW JDBC Password	Password for the user name.
Azure DW JDBC Schema Name	Name of the schema in the database.
Azure Storage Type	
Azure Blob Account Name	
Azure Blob Account Key	
ADLS Gen2 Storage Account Name	
ADLS Gen2 Account Key	
Blob End-Point	
VNet Rule	

**Note:** When you use a Microsoft SQL Server connection to access tables in a Microsoft SQL Server database, the Developer tool does not display the synonyms for the tables.

## Microsoft SQL Server Connection Properties

Use a Microsoft SQL Server connection to access tables in a Microsoft SQL Server database.

The following table describes the Microsoft SQL Server connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
Use Trusted Connection	Optional. When enabled, the Data Integration Service uses Windows authentication to access the Microsoft SQL Server database. The user name that starts the Data Integration Service must be a valid Windows user with access to the Microsoft SQL Server database.
Connection String for metadata access	Connection string to import physical data objects. Use the following connection string: <code>jdbc:informatica:sqlserver://&lt;host&gt;:&lt;port&gt;;databaseName=&lt;dbname&gt;</code>
Connection String for data access	Connection string to preview data and run mappings. Enter <code>&lt;ServerName&gt;@&lt;DBName&gt;</code>
Domain Name	Optional. Name of the domain where Microsoft SQL Server is running.
Packet Size	Required. Optimize the ODBC connection to Microsoft SQL Server. Increase the packet size to increase performance. Default is 0.
Code Page	Database code page.

Property	Description
Owner Name	Name of the schema owner. Specify for connections to the profiling warehouse database or data object cache database.
Schema Name	Name of the schema in the database. Specify for connections to the profiling warehouse or data object cache database. You must specify the schema name for the profiling warehouse if the schema name is different from the database user name. You must specify the schema name for the data object cache database if the schema name is different from the database user name and you manage the cache with an external tool.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

**Note:** When you use a Microsoft SQL Server connection to access tables in a Microsoft SQL Server database, the Developer tool does not display the synonyms for the tables.

## Oracle Connection Properties

Use an Oracle connection to access tables in an Oracle database.

The following table describes the Oracle connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.

Property	Description
Connection String for metadata access	<p>Connection string to import physical data objects.</p> <p>Use the following connection string: <code>jdbc:informatica:oracle://&lt;host&gt;:1521;SID=&lt;sid&gt;</code></p> <p>Use the following connection string to connect to Oracle through Oracle Connection Manager:</p> <p><code>jdbc:Informatica:oracle:TNSNamesFile=&lt;fully qualified path to the tnsnames.ora file&gt;;TNSServerName=&lt;TNS server name&gt;;</code></p>
Connection String for data access	Connection string to preview data and run mappings. Enter <code>dbname.world</code> from the TNSNAMES entry.
Code Page	Database code page.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Parallel Mode	Optional. Enables parallel processing when loading data into a table in bulk mode. Default is disabled.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

## PostgreSQL Connection Properties

Use a JDBC connection to access tables in a PostgreSQL database.

The following table describes the Oracle connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
JDBC Driver Class Name	

Property	Description
Connection String	Connection string to use to read data and metadata from the database. Define the connection string in the following format: <code>jdbc:informatica:postgresql://&lt;host&gt;:&lt;port&gt;;Database=&lt;id&gt;</code>
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Use Sqoop Connector	
Sqoop Arguments	

## Creating a Connection

In the Administrator tool, you can create relational database, social media, and file systems connections.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Connections** view.
3. In the Navigator, select the domain.
4. In the Navigator, click **Actions > New > Connection**.  
The **New Connection** dialog box appears.
5. In the **New Connection** dialog box, select the connection type, and then click **OK**.  
The **New Connection** wizard appears.
6. Enter the connection properties.  
The connection properties that you enter depend on the connection type. Click **Next** to go to the next page of the **New Connection** wizard.
7. When you finish entering connection properties, you can click **Test Connection** to test the connection.
8. Click **Finish**.

## CHAPTER 14

# Create and Configure Application Services

This chapter includes the following topics:

- [Checklist to Create and Configure Application Services, 255](#)
- [Create and Configure the Application Services Overview, 256](#)
- [Create and Configure the Model Repository Service, 256](#)
- [Create and Configure the Data Integration Service, 261](#)
- [Create and Configure the PowerCenter Repository Service, 264](#)
- [Create and Configure the PowerCenter Integration Service, 268](#)
- [Create and Configure the Metadata Manager Service, 270](#)
- [Create and Configure the Content Management Service, 274](#)
- [Create and Configure the Analyst Service, 276](#)
- [Create and Configure the Search Service, 278](#)

## Checklist to Create and Configure Application Services

This chapter contains instructions to create and configure application services. Even if you created services during installation, you might still need to configure some services. Use this checklist to track completion of application service configuration.

- ☐ Review your notes for planning the application services.
- ☐ Identify the services that you created during installation, and complete additional configuration for the service.
- ☐ Create and configure other services that you want in the domain.

# Create and Configure the Application Services Overview

If you did not create services with you ran the installer, use the Administrator tool to create the application services.

Some application services depend on other application services. When you create these dependent application services, you must provide the name of other running application services. Review the application service dependencies to determine the order that you must create the services. For example, you must create a Model Repository Service before you create a Data Integration Service.

Before you create the application services, verify that you have completed the prerequisite tasks required by the installation and configuration process.

## Create and Configure the Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services.

When you access a Model repository object from an Informatica client tool or application service, the client or service sends a request to the Model Repository Service. The Model Repository Service process fetches, inserts, and updates the metadata in the Model repository database tables.

### Create the Model Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Model Repository Service**.  
The **New Model Repository Service** dialog box appears.
3. On the **New Model Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.



Property	Description
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

- Click **Next**.

The **New Model Repository Service - Step 2 of 2** page appears.

- Enter the following properties for the Model repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository. You can enter the Windows NT user name for trusted connection for Microsoft SQL Server.
Password	Repository database password for the database user. You can enter the Windows NT password for trusted connection for Microsoft SQL Server.
Database Schema	Available for Microsoft SQL Server and PostgreSQL. Name of the schema that will contain Model repository tables.
Database Tablespace	Available for IBM DB2. Name of the tablespace in which to create the tables. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.

- Enter the JDBC connection string that the service uses to connect to the Model repository database.

Use the following syntax for the connection string for the selected database type:

Database Type	Connection String Syntax
IBM DB2	"jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000"
Microsoft SQL Server	<ul style="list-style-type: none"> <li>- <b>Microsoft SQL Server that uses the default instance</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft SQL Server that uses a named instance</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true"</li> <li>- <b>Microsoft Azure.</b> jdbc:informatica:sqlserver://&lt;host_name&gt;:&lt;port_number&gt;;DatabaseName=&lt;database_name&gt;;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.&lt;hostnameincertificate&gt;;ValidateServerCertificate=true</li> <li>- <b>Azure SQL Database with Active Directory authentication.</b> "jdbc:informatica: sqlserver://&lt;host_name&gt;:&lt;port_number&gt;;database=&lt;database_name&gt;;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostnameInCertificate=*.database.windows.net;loginTimeout=&lt;seconds&gt;"</li> </ul> <p><b>Note:</b> If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.</p> <ul style="list-style-type: none"> <li>- <b>Microsoft SQL Server that uses the default instance with Windows NT credentials:</b> "jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port number&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> <li>- <b>Microsoft SQL Server that uses a named instance with Windows NT credentials:</b> "jdbc:informatica:sqlserver://&lt;host name&gt;\&lt;named instance name&gt;;DatabaseName=&lt;database name&gt;;SnapshotSerializable=true;authenticationMethod=NTLM"</li> </ul>
Oracle	"jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"
PostgreSQL	"jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName= "

7. If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters in the **Secure JDBC Parameters** field.

Enter the parameters as name=value pairs separated by semicolon characters (;). For example:

```
param1=value1;param2=value2
```

Enter the following secure database parameters:

Secure Database Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to <code>SSL</code> .
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends.  If this parameter is set to <code>True</code> , Informatica validates the certificate that the database server sends. If you specify the <code>HostNameInCertificate</code> parameter, Informatica also validates the host name in the certificate.  If this parameter is set to <code>False</code> , Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify.
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to <code>cryptoProtocolVersion=TLSv1.1</code> or <code>cryptoProtocolVersion=TLSv1.2</code> based on the cryptographic protocol used by the database server.
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate for the database.  If you do not include the path for the truststore file, Informatica looks for the file in the following default directory: <code>&lt;Informatica installation directory&gt;/tomcat/bin</code>
TrustStorePassword	Required. Password for the truststore file for the secure database.

**Note:** Informatica appends the secure JDBC parameters to the JDBC connection string. If you include the secure JDBC parameters directly in the connection string, do not enter any parameter in the **Secure JDBC Parameters** field.

8. Click **Test Connection** to verify that you can connect to the database.
9. Select **No content exists under specified connection string. Create new content.**
10. Click **Finish**.

The domain creates the Model Repository Service, creates content for the Model repository in the specified database, and enables the service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the Model Repository Service

After you create the Model Repository Service, perform the following tasks:

- Create the Model repository user if the domain does not use Kerberos authentication.
- Create other application services.

## Create the Model Repository User

When you create an application service that depends on the Model Repository Service, you provide the name of the Model Repository Service and of this Model repository user.

If the domain does not use Kerberos authentication, the domain uses a user account to authenticate other application services that make requests to the Model Repository Service. You must create a user account and assign the user the Administrator role for the Model Repository Service.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create User** to create a native user account.

**Note:** If you set up LDAP authentication in the domain, you can use an LDAP user account for the Model repository user.

3. Enter the following properties for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > "
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > "

4. Click **OK**.  
The user properties appear.
5. Click the **Privileges** tab.
6. Click **Edit**.  
The **Edit Roles and Privileges** dialog box appears.
7. On the **Roles** tab, expand the Model Repository Service.
8. Under **System Defined Roles**, select Administrator and click **OK**.

## Create Other Services

After you create the Model Repository Service, create the application services that depend on the Model Repository Service.

Create the dependent services in the following order:

1. Data Integration Service
2. Analyst Service
3. Content Management Service
4. Search Service

# Create and Configure the Data Integration Service

When you preview or run data profiles, SQL data services, and mappings in the Analyst tool or the Developer tool, the client tool sends requests to the Data Integration Service to perform the data integration jobs. When you run SQL data services, mappings, and workflows from the command line program or an external client, the command sends the request to the Data Integration Service.

## Create the Data Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Data Integration Service, verify that you have created the following service:

Model Repository Service

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Domain Navigator, select the domain.
4. Click **Actions > New > Data Integration Service**.  
The **New Data Integration Service** wizard appears.
5. On the **New Data Integration Service - Step 1 of 14** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.

Property	Description
Assign	Select <b>Node</b> to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Next**.

The **New Data Integration Service - Step 2 of 14** page appears.

7. Enter the HTTP port number to use for the Data Integration Service.
8. Accept the default values for the remaining security properties. You can configure the security properties after you create the Data Integration Service.
9. Select **Enable Service**.

The Model Repository Service must be running to enable the Data Integration Service.

10. Verify that the **Move to plugin configuration page** is not selected.

11. Click **Next**.

The **New Data Integration Service - Step 3 of 14** page appears.

12. Set the **Launch Job Options** property to one of the following values:

- In the service process. Configure when you run SQL data service and web service jobs. SQL data service and web service jobs typically achieve better performance when the Data Integration Service runs jobs in the service process.
- In separate local processes. Configure when you run mapping, profile, and workflow jobs. When the Data Integration Service runs jobs in separate local processes, stability increases because an unexpected interruption to one job does not affect all other jobs.

If you configure the Data Integration Service to run on a grid after you create the service, you can configure the service to run jobs in separate remote processes.

13. Accept the default values for the remaining execution options and click **Next**.

The **New Data Integration Service - Step 4 of 14** page appears.

14. If you created the data object cache database for the Data Integration Service, click **Select** to select the cache connection. Select the data object cache connection that you created for the service to access the database.

15. Accept the default values for the remaining properties on this page and click **Next**.

The **New Data Integration Service - Step 5 of 14** page appears.

16. For optimal performance, enable the Data Integration Service modules that you plan to use.

The following table lists the Data Integration Service modules that you can enable:

Module	Description
Web Service Module	Runs web service operation mappings.
Mapping Service Module	Runs mappings and previews.
Profiling Service Module	Runs profiles and scorecards.
SQL Service Module	Runs SQL queries from a third-party client tool to an SQL data service.
Workflow Orchestration Service Module	Runs workflows.

17. Click **Next**.

The **New Data Integration Service - Step 6 of 14** page appears.

You can configure the HTTP proxy server properties to redirect HTTP requests to the Data Integration Service. You can configure the HTTP configuration properties to filter the web services client machines that can send requests to the Data Integration Service. You can configure these properties after you create the service.

18. Accept the default values for the HTTP proxy server and HTTP configuration properties and click **Next**.

The **New Data Integration Service - Step 7 of 14** page appears.

The Data Integration Service uses the result set cache properties to use cached results for SQL data service queries and web service requests. You can configure the properties after you create the service.

19. Accept the default values for the result set cache properties and click **Next**.

The **New Data Integration Service - Step 8 of 14** page appears.

20. If you created the profiling warehouse database for the Data Integration Service, select the Profiling Service module.

21. If you created the workflow database for the Data Integration Service, select the Workflow Orchestration Service module.

22. Verify that the remaining modules are not selected.

You can configure properties for the remaining modules after you create the service.

23. Click **Next**.

The **New Data Integration Service - Step 11 of 14** page appears.

24. If you created the profiling warehouse database for the Data Integration Service, click **Select** to select the database connection. Select the profiling warehouse connection that you created for the service to access the database.

25. Select whether or not content exists in the profiling warehouse database.

If you created a new profiling warehouse database, select **No content exists under specified connection string**.

26. Click **Next**.

The **New Data Integration Service - Step 12 of 14** page appears.

27. Accept the default values for the advanced profiling properties and click **Next**.

The **New Data Integration Service - Step 14 of 14** page appears.

28. If you created the workflow database for the Data Integration Service, click **Select** to select the database connection. Select the workflow database connection that you created for the service to access the database.

29. Click **Finish**.

The domain creates and enables the Data Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the Data Integration Service

After you create the Data Integration Service, perform the following tasks:

- Verify the host file configuration.
- Create other application services.

### Verify the Host File Configuration

If you configured the Data Integration Service on UNIX or Linux to launch jobs as separate processes, verify that the host file on the node that runs the service contains a localhost entry. Otherwise, jobs fail when the **Launch Jobs as Separate Processes** property for the Data Integration Service is enabled.

### Create Other Services

After you create the Data Integration Service, create the application services that depend on the Data Integration Service.

Create the dependent services in the following order:

1. Content Management Service
2. Analyst Service
3. Search Service

## Create and Configure the PowerCenter Repository Service

The PowerCenter Repository Service is an application service that manages the PowerCenter repository. The PowerCenter repository stores metadata created by the PowerCenter Client and application services in a relational database.

When you access a PowerCenter repository object from the PowerCenter Client or the PowerCenter Integration Service, the client or service sends a request to the PowerCenter Repository Service. The PowerCenter Repository Service process fetches, inserts, and updates metadata in the PowerCenter repository database tables.



## Create the PowerCenter Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.

2. Click **Actions > New > PowerCenter Repository Service**.

The **New PowerCenter Repository Service** dialog box appears.

3. On the **New PowerCenter Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.

The **New PowerCenter Repository Service - Step 2 of 2** page appears.

5. Enter the following properties for the PowerCenter repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	Password for the PowerCenter repository database user. Must be in 7-bit ASCII.
Connection String	Native connection string the PowerCenter Repository Service uses to access the repository database. Use the following native connect string syntax for each supported database: <ul style="list-style-type: none"><li>- servername@databasename for Microsoft SQL Server and Sybase.</li><li>- databasename.world for Oracle.</li><li>- databasename for IBM DB2.</li></ul>

Property	Description
Code Page	Repository database code page. The PowerCenter Repository Service uses the character set encoded in the database code page to write data. You cannot change the code page in the PowerCenter Repository Service properties after you create the PowerCenter Repository Service.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 and Sybase databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.

6. Select **No content exists under specified connection string. Create new content.**
7. Optionally, choose to create a global repository.  
After you create the service, you can promote a local repository to a global repository, but you cannot change a global repository to a local repository.
8. If your license has the team-based development option, you can optionally enable version control of the repository.  
After you create the service, you can convert a non-versioned repository to a versioned repository, but you cannot convert a versioned repository to a non-versioned repository.
9. Click **Finish**.  
The domain creates the PowerCenter Repository Service, starts the service, and creates content for the PowerCenter repository.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the PowerCenter Repository Service

After you create the PowerCenter Repository Service, perform the following tasks:

- Configure the PowerCenter Repository Service to run in the Normal mode.
- Create the PowerCenter repository user if the domain does not use Kerberos authentication.
- Create other application services.

### Run the PowerCenter Repository Service in Normal Mode

After you create the PowerCenter Repository Service, it starts in exclusive mode and access is restricted to the administrator. Edit the service properties to run the service in normal operating mode to provide access to other users.

1. In the Administrator tool, click the **Manage** tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. Click **Properties**.
4. Click **Edit Repository Properties**.
5. In the **Operating Mode** field, select Normal.
6. Click **OK**.  
You must recycle the PowerCenter Repository Service for the changes to take effect.
7. Select **Actions > Recycle Service**.

## Create the PowerCenter Repository User

If the domain does not use Kerberos authentication, the domain uses a user account to authenticate other application services that make requests to the PowerCenter Repository Service. You must create a user account and assign the user the Administrator role for the PowerCenter Repository Service.

When you create an application service that depends on the PowerCenter Repository Service, you provide the name of the PowerCenter Repository Service and of this PowerCenter repository user.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create User** to create a native user account.

**Note:** If you set up LDAP authentication in the domain, you can use an LDAP user account for the PowerCenter repository user.

3. Enter the following properties for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > "
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > "

4. Click **OK**.  
The user properties appear.
5. Click the **Privileges** tab.
6. Click **Edit**.  
The **Edit Roles and Privileges** dialog box appears.
7. On the **Roles** tab, expand the PowerCenter Repository Service.
8. Under **System Defined Roles**, select Administrator and click **OK**.

## Create Other Services

After you create the PowerCenter Repository Service, create the application services that depend on the PowerCenter Repository Service.

You can create the following application services:

1. PowerCenter Integration Service
2. Metadata Manager Service
3. Web Services Hub Service

# Create and Configure the PowerCenter Integration Service

The PowerCenter Integration Service is an application service that runs workflows and sessions for the PowerCenter Client.

When you run a workflow in the PowerCenter Client, the client sends the requests to the PowerCenter Integration Service. The PowerCenter Integration Service connects to the PowerCenter Repository Service to fetch metadata from the PowerCenter repository, and then runs and monitors the sessions and workflows.

## Create the PowerCenter Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the PowerCenter Integration Service, verify that you created the following service:

PowerCenter Repository Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > PowerCenter Integration Service**.  
The **New PowerCenter Integration Service** dialog box appears.
3. On the **New PowerCenter Integration Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

Property	Description
Assign	Select <b>Node</b> to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.
5. On the **New PowerCenter Integration Service - Step 2 of 2** page, enter the following properties:

Property	Description
PowerCenter Repository Service	PowerCenter Repository Service you want to associate with the service.
Username	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.
Password	Password associated with the PowerCenter repository user. Not available for a domain with Kerberos authentication.
Security Domain	LDAP security domain for the PowerCenter repository user. The <b>Security Domain</b> field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

6. Select the data movement mode that determines how the PowerCenter Integration Service handles character data. Choose ASCII or Unicode. Default is ASCII.  
  
In ASCII mode, the PowerCenter Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. In Unicode mode, the PowerCenter Integration Service recognizes multibyte character sets as defined by the supported code pages. Use Unicode mode when the sources or targets use 8-bit or multibyte character sets and contain character data.
7. Click **Finish**.
8. On the **Specify Code Pages** dialog box, assign a code page for the PowerCenter Integration Service.  
  
The code page for the PowerCenter Integration Service must be compatible with the code page of the associated repository.
9. Click **OK**.  
  
The domain creates the PowerCenter Integration Service. The domain does not enable the PowerCenter Integration Service during the service creation process.
10. To enable the PowerCenter Integration Service, select the service in the Navigator, and click **Actions** > **Enable Service**. The PowerCenter Repository Service must be running to enable the PowerCenter Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the PowerCenter Integration Service

After you create the PowerCenter Integration Service, create the Metadata Manager Service that depends on the PowerCenter Integration Service.

## Create and Configure the Metadata Manager Service

The Metadata Manager Service is an application service that runs the Metadata Manager web client in the Informatica domain. The Metadata Manager Service manages the connections between service components and the users that have access to Metadata Manager.

When you load metadata into the Metadata Manager warehouse, the Metadata Manager Service connects to the PowerCenter Integration Service. The PowerCenter Integration Service runs workflows in the PowerCenter repository to read from metadata sources and load metadata into the Metadata Manager warehouse. When you use Metadata Manager to browse and analyze metadata, the Metadata Manager Service accesses the metadata from the Metadata Manager repository.

### Create the Metadata Manager Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Metadata Manager Service, verify that you created and enabled the following services:

PowerCenter Repository Service

PowerCenter Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Metadata Manager Service**.  
The **New Metadata Manager Service** dialog box appears.
3. On the **New Metadata Manager Service - Step 1 of 3** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Specify the following properties of the associated repository service:

Property	Description
Associated Integration Service	Select the PowerCenter Integration Service used by Metadata Manager to load metadata into the Metadata Manager warehouse.
Repository User Name	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.
Repository Password	Password associated with the PowerCenter repository user. Not available for a domain with Kerberos authentication.
Security Domain	LDAP security domain for the PowerCenter repository user. The <b>Security Domain</b> field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

5. Click **Next**.

The **New Metadata Manager Service - Step 2 of 3** page appears.

6. Enter the following database properties for the Metadata Manager repository:

Property	Description
Database Type	The type of the repository database.
Code Page	Metadata Manager repository code page. The Metadata Manager Service and the Metadata Manager application use the character set encoded in the repository code page when writing data to the Metadata Manager repository. You can enable the Metadata Manager Service only after you specify the code page.
Connect String	Native connect string to the Metadata Manager repository database. The Metadata Manager Service uses the connect string to create a connection object to the Metadata Manager repository in the PowerCenter repository. Use the following native connect string syntax for each supported database: <ul style="list-style-type: none"><li>- <code>servername@databasename</code> for Microsoft SQL Server.</li><li>- <code>databasename.world</code> for Oracle.</li><li>- <code>databasename</code> for IBM DB2.</li></ul>
Database User	The database user name for the repository.
Database Password	Password for the Metadata Manager repository database user. Must be in 7-bit ASCII.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.

Property	Description
Database Hostname	The name of the machine that hosts the database server.
Database Port	The port number on which you configure the database server listener service.
SID/Service Name	For Oracle databases. Indicates whether to use the SID or service name in the JDBC connection string. For Oracle RAC databases, select from Oracle SID or Oracle service name. For other Oracle databases, select Oracle SID.
Database Name	The name of the database server. Specify the full service name or SID for Oracle databases, service name for IBM DB2 databases, and database name for Microsoft SQL Server databases.

7. If you want to append parameters to the database connection URL, configure additional parameters in the **Additional JDBC Parameters** field. Enter the parameters as name=value pairs separated by semicolon characters (;). For example: param1=value1;param2=value2

You can use this property to specify the following parameters:

Parameter	Description
Backup server location	If you use a database server that is highly available such as Oracle RAC, enter the location of a backup server.
Oracle Advanced Security Option (ASO) parameters	<p>If the Metadata Manager repository database is an Oracle database that uses ASO, enter the following additional parameters:</p> <pre>EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]</pre> <p><b>Note:</b> The parameter values must match the values in the <code>sqlnet.ora</code> file on the machine where the Metadata Manager Service runs.</p>
Authentication information for Microsoft SQL Server	<p>To authenticate the user credentials with Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, enter the following text:</p> <pre>AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]. jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name]; AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]</pre> <p>When you use a trusted connection to connect to a Microsoft SQL Server database, the Metadata Manager Service connects to the repository with the credentials of the user logged in to the machine on which the service is running.</p> <p>To start the Metadata Manager Service as a Windows service with a trusted connection, configure the Windows service properties to log on with a trusted user account.</p>

8. If the Metadata Manager repository database is configured for secure communication, you can configure additional JDBC parameters in the **Secure JDBC Parameters** field.

Use this property to specify secure connection parameters such as passwords. The Administrator tool does not display secure parameters or parameter values in the Metadata Manager Service properties.



Enter the parameters as name=value pairs separated by semicolon characters (;). For example:

param1=value1;param2=value2.

Enter the following secure database parameters:

Secure Database Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to <code>SSL</code> .
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate of the database server.
TrustStorePassword	Required. Password used to access the truststore file.
HostNameInCertificate	Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the SSL certificate.
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends.  If this parameter is set to <code>True</code> , Informatica validates the certificate that the database server sends. If you specify the <code>HostNameInCertificate</code> parameter, Informatica also validates the host name in the certificate.  If this parameter is set to <code>False</code> , Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify.
KeyStore	Path and file name of the keystore file that contains the SSL certificates that the Metadata Manager Service sends to the database server.
KeyStorePassword	Password used to access the keystore file.

9. Click **Next**.

The **New Metadata Manager Service - Step 3 of 3** page appears.

10. Enter the HTTP port number to use for the service.

11. To enable secure communications with the Metadata Manager Service, select **Enable Secured Socket Layer**.

Enter the following properties to configure secure communication for the service:

Property	Description
HTTPS Port	Port number to use for a secure connection to the service. Use a different port number than the HTTP port number.
Keystore File	Path and file name of the keystore file that contains the private or public key pairs and associated certificates. Required if you use HTTPS connections for the service.
Keystore Password	Plain-text password for the keystore file.

12. Click **Finish**.

The domain creates the Metadata Manager Service. The domain does not enable the Metadata Manager Service during the service creation process.

13. To enable the Metadata Manager Service, select the service in the Navigator and click **Actions > Enable Service**. The PowerCenter Repository Service and PowerCenter Integration Service must be running to enable the Metadata Manager Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the Metadata Manager Service

After you create the Metadata Manager Service, perform the following tasks:

- Create the contents for the Metadata Manager repository.
- Create other application services.

When you create the Metadata Manager Service, you create the repository tables and import models for metadata sources.

1. In the Navigator, select the Metadata Manager Service.
2. Click **Actions > Repository Contents > Create**.
3. Click **OK**.

After you create the Metadata Manager Service, create the application services that depend on the Metadata Manager Service.

## Create and Configure the Content Management Service

The Content Management Service is an application service that manages reference data. A reference data object contains a set of data values that you can search while performing data quality operations on source data. The Content Management Service also compiles rule specifications into mapplets. A rule specification object describes the data requirements of a business rule in logical terms.

The Content Management Service uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. The Content Management Service also provides transformations, mapping specifications, and rule specifications with the following types of reference data:

- Address reference data
- Identity populations
- Probabilistic models and classifier models
- Reference tables

## Create the Content Management Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Content Management Service, verify that you have created and enabled the following services:

Model Repository Service  
Data Integration Service

1. In the Administrator tool, click the **Manage** tab.

2. Click **Actions > New > Content Management Service**.

The **New Content Management Service** dialog box appears.

3. On the **New Content Management Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
HTTP Port	HTTP port number to use for the Content Management Service.
Data Integration Service	Data Integration Service to associate with the service. The Data Integration Service and the Content Management Service must run on the same node.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.
Reference Data Location	Reference data warehouse connection that you created for the Content Management Service to access the reference data warehouse. Click <b>Select</b> to select the connection.

4. Click **Next**.

The **New Content Management Service - Step 2 of 2** page appears.

5. Accept the default values for the security properties.

6. Select **Enable Service**.

The Model Repository Service and Data Integration Service must be running to enable the Content Management Service.

7. Click **Finish**.

The domain creates and enables the Content Management Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

# Create and Configure the Analyst Service

The Analyst Service is an application service that runs the Analyst tool in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to the Analyst tool.

## Create the Analyst Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Analyst Service, verify that you have created and enabled the following services:

Model Repository Service

Data Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Analyst Service**.  
The **New Analyst Service** dialog box appears.
3. On the **New Analyst Service - Step 1 of 6** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Click **Next**.  
The **New Analyst Service - Step 2 of 6** page appears.
5. Enter the HTTP port number to use for communication from the Analyst tool to the Analyst Service.
6. To enable secure communication from the Analyst tool to the Analyst Service, select **Enable Secure Communication**.

Enter the following properties to configure secure communication for the Analyst Service:

Property	Description
HTTPS Port	Port number that the Analyst tool runs on when you enable secure communication. Use a different port number than the HTTP port number.
Keystore File	Directory where the keystore file that contains the digital certificates is stored.
Keystore Password	Plain-text password for the keystore file. If this property is not set, the Analyst Service uses the default password <code>changeit</code> .
SSL Protocol	Optional. Indicates the protocol to be used. Set this property to <code>SSL</code> .

7. Select **Enable Service**.

The Model Repository Service and the Data Integration Service must be running to enable the Analyst Service.

8. Click **Next**.

The **New Analyst Service - Step 3 of 6** page appears.

9. Enter the following properties to associate the Model Repository Service with the Analyst Service:

Description	Property
Model Repository Service	Model Repository Service to associate with the service.
User name	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

10. To enable Analyst tool users to work on Human task data, set the **Data Integration Service** property to the Data Integration Service that you configure to run workflows.

If Analyst tool users do not need to work on Human task records, do not configure this property.

11. Click **Next**.

The **New Analyst Service - Step 4 of 6** page appears.

12. Enter the following run-time properties for the Analyst Service:

Property	Description
Data Integration Service	Data Integration Service to associate with the service. The Analyst Service manages the connection to the Data Integration Service that enables users to perform data preview, mapping specification, scorecard, and profile jobs in the Analyst tool.  You can associate the Analyst Service with the Data Integration Service that you configured to run workflows. Or, you can associate the Analyst Service with different Data Integration Services for the different operations.
Flat File Cache Directory	Directory of the flat file cache where the Analyst tool stores uploaded flat files. The Data Integration Service must also be able to access this directory. If the Analyst Service and the Data Integration Service run on different nodes, configure the flat file directory to use a shared directory.

13. Click **Next**.

The **New Analyst Service - Step 5 of 6** page appears.

14. Enter the directory to store the temporary business glossary files that the business glossary export process creates and the directory to store files that content managers attach to the Glossary assets. These directories must be on the node that runs the Analyst Service.

15. Click **Finish**.

The domain creates and enables the Analyst Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the Analyst Service

After you create the Analyst Service, create the Search Service that depends on the Analyst Service.

# Create and Configure the Search Service

The Search Service performs searches in the Analyst tool. It returns search results from the profiling warehouse and the Model repository, including data objects, mapping specifications, and scorecards

By default, the Search Service returns search results from a Model repository, such as data objects, mapping specifications, profiles, reference tables, rules, scorecards, and business glossary terms. The search results can also include column profile results and domain discovery results from a profiling warehouse.

## Create the Search Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Search Service, verify that you have created and enabled the following services:

- Model Repository Service
- Data Integration Service
- Analyst Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Search Service**.  
The **New Search Service** dialog box appears.
3. On the **New Search Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Click **Next**.  
The **New Search Service - Step 2 of 2** page appears.
5. Enter the following search properties for the Search Service:

Description	Property
Port Number	Port number to use for the Search Service.
Index Location	Directory that contains the search index files. Enter a directory on the machine that runs the Search Service. If the directory does not exist, Informatica creates the directory when it creates the Search Service.
Extraction Interval	Interval in seconds at which the Search Service extracts and indexes updated content. Default is 60 seconds.
Model Repository Service	Model Repository Service to associate with the service.
User Name	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Finish**.  
The domain creates the Search Service. The domain does not enable the Search Service during the creation process. You must enable the Search Service before users can perform searches in the Analyst tool and Business Glossary Desktop.

7. To enable the Search Service, select the service in the Navigator, and then click **Actions > Enable Service**.

The Model Repository Service, Data Integration Service, and Analyst Service must be running to enable the Search Service.

After you create the service through the wizard, you can edit the properties or configure other properties.



# Part V: Informatica Client Installation

This part contains the following chapters:

- [Install the Clients, 282](#)
- [Install in Silent Mode , 289](#)

## CHAPTER 15

# Install the Clients

This chapter includes the following topics:

- [Install the Clients Overview, 282](#)
- [Before You Install, 283](#)
- [Install the Clients, 284](#)
- [After You Install, 285](#)
- [Starting the PowerCenter Client, 287](#)
- [Starting the Developer Tool, 287](#)

## Install the Clients Overview

You can install the Informatica clients on Windows in graphical or silent mode.

Complete the pre-installation tasks to prepare for the installation. You can install the Informatica clients on multiple machines.

When you run the client installer, you can select the following Informatica client tools:

### **Informatica Developer**

Informatica Developer is a client application that you use to create data objects, create and run mappings, and create virtual databases.

### **PowerCenter Client**

The PowerCenter Client is a set of tools you can use to manage the PowerCenter repository, mappings, and sessions.

**Note:** Informatica recommends that you install the Informatica services and the PowerCenter Client in different install directories. If you install the Informatica services and the PowerCenter Client in the same install directory, the service binaries will be uninstalled when you uninstall the PowerCenter Client.

# Before You Install

Before you install the Informatica clients on Windows, verify that the minimum system and third-party software requirements are met. If the machine where you install the Informatica clients is not configured correctly, the installation can fail.

## Verify Installer Package Checksum

Before you run the client installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installer.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

The following table lists the checksum and file size for Informatica client on Windows:

File	Checksum Value	File Size
informatica_1053_client_winem-64t.zip	590321451	3139423400

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see [HOW TO: Identify file errors after downloading Informatica installation files](#).

## Verify System Requirements

Before you install the client, verify the following installation requirements to install and run the client are met:

### Disk space for the temporary files

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

### Permissions to install

Verify that the user account that you use to install the client has write permission on the installation directory and Windows registry.

### Minimum system requirements

The following table lists the minimum system requirements to run the client:

Processor	RAM	Disk Space
1 CPU	1GB	6 GB

## Verify Third-party Requirements for Informatica Developer

Before you install the Developer tool, verify the following third-party installation requirements:

- Install the .NET Framework 4.0 or later. If you plan to use Data Processor or Hierarchical-To-Relational transformations, you must install the .NET Framework before you install the Developer tool.

- Install the latest version of Microsoft Visual C++ Redistributable Package (x64) before you use or install the Developer tool. You can download it from the Microsoft website.

## Verify Third-party Requirements for the PowerCenter Client

The PowerCenter Client installation includes Mapping Architect for Visio and Mapping Analyst for Excel. Verify third-party requirements for both Mapping Architect for Visio and Mapping Analyst for Excel before you install the PowerCenter Client.

### Verify Third-party Requirements for Mapping Architect for Visio

If you plan to use Mapping Architect for Visio, install the following third-party software before you install the PowerCenter Client:

- Microsoft Visio version 2007 or 2010
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.0

**Important:** If you do not install the correct version and service pack level of Microsoft .NET Framework, Mapping Architect for Visio will not install properly.

### Verify Third-party Requirements for Mapping Analyst for Excel

Mapping Analyst for Excel includes an Excel add-in that adds a Metadata menu or ribbon to Microsoft Excel. You can install the add-in only for Excel 2016. If you plan to use Mapping Analyst for Excel, install the following third-party software before you install the PowerCenter Client:

- Microsoft Office Excel version 2016
- Java version 1.8 or later

## Install the Clients

Perform the following steps to install the client tool:

1. Close all other applications.
2. Go to the root of the directory for the installation files and run install.bat as administrator.

To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

**Note:** If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

If you encounter problems when you run the install.bat file from the root directory, run the following file:

```
<installer files directory>\client\install.exe
```

3. Select **Install Informatica <Version> Clients** and click **Next**.
4. The **Installation Pre-requisites** page displays the system requirements. Verify that all installation requirements are met before you continue the installation.
5. On the **Installation Directory** page, enter the absolute path for the installation directory.

The installation directory must be on the current computer. The maximum length of the path must be less than 260 characters. The directory names in the path must not contain spaces or the following special characters: @|\* \$ # ! % ( ) { } [ ] , ; ' .

**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

6. If you want to install distribution packages through the Informatica installer, select the check box.
7. If you choose to install distribution packages, select one or more packages from the list that you want to install.
8. Click **Next**.
9. On the **Pre-Installation Summary** page, review the installation information, and click **Install**.  
The installer copies the Developer tool files to the installation directory.  
The **Post-installation Summary** page indicates whether the installation completed successfully.
10. Click **Done** to close the installer.

You can view the installation log files to get more information about the tasks performed by the installer.

## After You Install

After you install the client tools, you can install other languages, enable secure communication within the domain and start the tool.

### Install Languages

To view languages other than the system locale and to work with repositories that use a UTF-8 code page, install additional languages on Windows for use with the Informatica clients.

**Note:** If you installed the PowerCenter clients and performed this install languages task, you do not need to repeat the task.

You also must install languages to use the Windows Input Method Editor (IME).

1. Click **Start > Settings > Control Panel**.
2. Click **Regional Options**.
3. Under Language settings for the system, select the languages you want to install.
4. Click **Apply**.

If you change the system locale when you install the language, restart the Windows machine.

### Configure the Client for a Secure Domain

When you enable secure communication within the domain, you also secure connections between the domain and Informatica client applications. Based on the truststore files used, you might need to specify the location and password for the truststore files in environment variables on each client host.

You might need to set the following environment variables on each client host:

#### **INFA\_TRUSTSTORE**

Set this variable to the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named `infa_truststore.jks` and `infa_truststore.pem`.

## INFA\_TRUSTSTORE\_PASSWORD

Set this variable to the password for the `infa_truststore.jks` file. The password must be encrypted. Use the command line program `mpasswd` to encrypt the password.

Informatica provides an SSL certificate that you can use to secure the domain. When you install the Informatica clients, the installer sets the environment variables and installs the truststore files in the following directory by default: `<Informatica installation directory>\clients\shared\security`

If you use the default Informatica SSL certificate, and the `infa_truststore.jks` and `infa_truststore.pem` are in the default directory, you do not need to set the `INFA_TRUSTSTORE` or `INFA_TRUSTSTORE_PASSWORD` environment variables.

You must set the `INFA_TRUSTSTORE` and `INFA_TRUSTSTORE_PASSWORD` environment variables on each client host in the following scenarios:

### You use a custom SSL certificate to secure the domain.

If you provide an SSL certificate to use to secure the domain, copy the `infa_truststore.jks` and `infa_truststore.pem` truststore files to each client host. You must specify the location of the files and the truststore password.

### You use the default Informatica SSL certificate, but the truststore files are not in the default Informatica directory.

If you use the default Informatica SSL certificate, but the `infa_truststore.jks` and `infa_truststore.pem` truststore files are not in the default Informatica directory, you must specify the location of the files and the truststore password.

## Configure the Developer Tool Workspace Directory

Configure Informatica Developer to write the workspace metadata to the machine where the user is logged in.

**Note:** If you have installed the PowerCenter clients and performed this task, you do not need to repeat this task.

1. Go to the following directory: `<Informatica installation directory>\clients\DeveloperClient\configuration\`
2. Locate the `config.ini` file.
3. Create a backup copy of the `config.ini` file.
4. Use a text editor to open the `config.ini` file.
5. Add the `osgi.instance.area.default` variable to the end of the `config.ini` file and set the variable to the directory location where you want to save the workspace metadata. The file path cannot contain non-ANSI characters. Folder names in the workspace directory cannot contain the number sign (#) character. If folder names in the workspace directory contain spaces, enclose the full directory in double quotes.

- If you run Informatica Developer from the local machine, set the variable to the absolute path of the workspace directory:

```
osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
```

or

```
osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
```

- If you run Informatica Developer from a remote machine, set the variable to the directory location on the local machine:

```
osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
```

or

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

The user must have write permission to the local workspace directory.

Informatica Developer writes the workspace metadata to the workspace directory. If you log into Informatica Developer from a local machine, Informatica Developer writes the workspace metadata to the local machine. If the workspace directory does not exist on the machine from which you logged in, Informatica Developer creates the directory when it writes the files.

You can override the workspace directory when you start Informatica Developer.

## Starting the PowerCenter Client

When you start PowerCenter Client, you connect to a PowerCenter repository.

1. From the Windows Start menu, click **Programs > Informatica[Version] > Client > [Client Tool Name]**.

The first time you run a PowerCenter Client tool, you must add a repository and connect to it.

2. Click **Repository > Add Repository**.

The **Add Repository** dialog box appears.

3. Enter the repository and user name.

4. Click **OK**.

The repository appears in the Navigator.

5. Click **Repository > Connect**.

The Connect to Repository dialog box appears.

6. In the connection settings section, click **Add** to add the domain connection information.

The **Add Domain** dialog box appears.

7. Enter the domain name, gateway host, and gateway port number.

8. Click **OK**.

9. In the **Connect to Repository** dialog box, enter the password for the Administrator user.

10. Select the security domain.

11. Click **Connect**.

After you connect to the repository, you can create objects.

## Starting the Developer Tool

When you start the Developer tool, you connect to a Model repository. The Model repository stores metadata created in the Developer tool. The Model Repository Service manages the Model repository. Connect to the repository before you create a project.

1. From the Windows Start menu, click **Programs > Informatica[Version] > Client > Developer Client > Launch Informatica Developer**.

The first time you run the Developer tool, the Welcome page displays several icons. The Welcome page does not appear when you run the Developer tool subsequently.

2. Click **Workbench**.

The first time you start the Developer tool, you must select the repository in which to save the objects you create.

3. Click **File > Connect to Repository**.

The **Connect to Repository** dialog box appears.

4. If you have not configured a domain in the Developer tool, click **Configure Domains** to configure a domain.

You must configure a domain to access a Model Repository Service.

5. Click **Add** to add a domain.

The **New Domain** dialog box appears.

6. Enter the domain name, host name, and port number.

7. Click **Finish**.

8. Click **OK**.

9. In the **Connect to Repository** dialog box, click **Browse** and select the Model Repository Service.

10. Click **OK**.

11. Click **Next**.

12. Enter a user name and password.

13. Click **Finish**.

The Developer tool adds the Model repository to the Object Explorer view. When you run the Developer tool the next time, you can connect to the same repository.



## CHAPTER 16

# Install in Silent Mode

This chapter includes the following topics:

- [Overview of Install in Silent Mode, 289](#)
- [Configure the Properties File, 289](#)
- [Run the Silent Installer, 290](#)

## Overview of Install in Silent Mode

To install the Informatica clients without user interaction, install in silent mode.

Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the Informatica clients on multiple machines on the network or to standardize the installation across machines.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.

## Configure the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample `SilentInput.properties` file is stored in the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the `SilentInput.properties` file.
4. Use a text editor to open and modify the values of the properties in the file.

The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.
INSTALL_HADOOP_LIBRARIES	Determines whether to install distribution packages through the installer. Set the value to true if you want to install distribution packages through the installer. Set the value to false if you don't need distribution packages or if you want to install them later.
SELECTED_HADOOP_LIBRARIES	Determines the distribution packages that you want to install from the supported packages list. Enter the distribution packages that you want to install, separating multiple packages with a comma.

5. Save the properties file.

## Run the Silent Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file SilentInput.properties that you edited and resaved.
4. To run the silent installation, run silentInstall.bat.

The silent installer runs in the background. The process can take a while. The silent installation is complete when the Informatica\_<Version>\_Client\_InstallLog<timestamp>.log file is created in the installation directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

# Part VI: Uninstallation

This part contains the following chapter:

- [Uninstallation, 292](#)

## CHAPTER 17

# Uninstallation

This chapter includes the following topics:

- [Informatica Uninstallation Overview, 292](#)
- [Rules and Guidelines for Uninstallation, 292](#)
- [Uninstalling the Informatica Server in Console Mode, 293](#)
- [Uninstalling Informatica Server in Silent Mode, 293](#)
- [Uninstalling the Informatica Server in Graphical Mode, 294](#)
- [Informatica Client Uninstallation, 294](#)

## Informatica Uninstallation Overview

Uninstall Informatica to remove the Informatica server or clients from a machine.

The Informatica uninstallation process deletes all Informatica files and clears all Informatica configurations from a machine. The uninstallation process does not delete files that are not installed with Informatica. For example, the installation process creates temporary directories. The uninstaller does not keep a record of these directories and therefore cannot delete them. You must manually delete these directories for a clean uninstallation.

**Important:** If you install the Informatica services and the PowerCenter Client in the same install directory, the service binaries will be uninstalled when you uninstall the PowerCenter Client.

## Rules and Guidelines for Uninstallation

Use the following rules and guidelines when you uninstall Informatica components:

- The Informatica server uninstallation mode depends on the mode you use to install Informatica server. For example, you install Informatica server in console mode. When you run the uninstaller, it runs in console mode. The Informatica clients uninstallation mode does not depend on the mode you use to install Informatica clients. For example, you install Informatica clients in silent mode. When you run the uninstaller, it can run in graphical or silent mode.
- Uninstalling Informatica does not affect the Informatica repositories. The uninstaller removes the Informatica files. It does not remove repositories from the database. If you need to move the repositories, you can back them up and restore them to another database.

- Uninstalling Informatica does not remove the metadata tables from the domain configuration database. If you install Informatica again using the same domain configuration database and user account, you must manually remove the tables or choose to overwrite the tables. You can use the `infasetup BackupDomain` command to back up the domain configuration database before you overwrite the metadata tables. To remove the metadata tables manually, use the `infasetup DeleteDomain` command before you run the uninstaller.
- Uninstalling Informatica removes all installation files and subdirectories from the Informatica installation directory. Before you uninstall Informatica, stop all Informatica services and processes and verify that all of the files in the installation directory are closed. At the end of the uninstallation process, the uninstaller displays the names of the files and directories that could not be removed.
- The Informatica server installation creates the following folder for the files and libraries required by third party adapters built using the Informatica Development Platform APIs:  
`<Informatica installation directory>/services/shared/extensions`  
 Uninstalling the Informatica server deletes this folder and any subfolders created under it. If you have adapter files stored in the `/extensions` folder, back up the folder before you start uninstallation.
- If you perform the uninstallation on a machine, you must back up the ODBC folder before you uninstall. Restore the folder after the uninstallation completes.

## Uninstalling the Informatica Server in Console Mode

If you installed the Informatica server in console mode, uninstall the Informatica server in console mode.

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Go to the following directory:  
`<Informatica installation directory>/Uninstaller_Server`
2. Type the following command to run the uninstaller:  
`./uninstaller.sh`

If you installed the Informatica server in console mode, the uninstaller launches in console mode.

## Uninstalling Informatica Server in Silent Mode

If you installed the Informatica server in silent mode, uninstall the Informatica server in silent mode.

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Go to the following directory:  
`<Informatica installation directory>/Uninstaller_Server`
2. Type the following command to run the silent uninstaller:  
`./uninstaller.sh`

If you installed the Informatica server in silent mode, the uninstaller launches in silent mode. The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if the installation directory is not accessible.

After you uninstall the the Informatica server, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica\_<Version>\_Services\_InstallLog.log file
- Informatica\_<Version>\_Services\_<timestamp>.log file

## Uninstalling the Informatica Server in Graphical Mode

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Click **Start > Program Files > Informatica [Version] > Server > Uninstaller**.

The **Uninstallation** page appears.

2. Click **Uninstall** to begin the uninstallation.

After the installer deletes all of the Informatica files from the directory, the **Post-Uninstallation Summary** page appears.

3. Click **Done** to close the uninstaller.

After you uninstall the the Informatica server, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica\_<Version>\_Client\_InstallLog.log file
- Informatica\_<Version>\_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

## Informatica Client Uninstallation

You can uninstall the Informatica clients in graphical mode and silent mode on Windows.

When you uninstall Informatica clients, the installer does not remove the environment variables, INFA\_TRUSTSTORE, that it creates during installation. When you install a later version of Informatica clients, you must edit the environment variable to point to the new value of the SSL certificate.

### Uninstalling Informatica Clients in Graphical Mode

If you installed the Informatica clients in graphical mode, uninstall the Informatica clients in graphical mode.

1. Click **Start > Program Files > Informatica [Version] > Client > Uninstaller**.

The **Uninstallation** page appears.

2. Click **Next**.

The **Application Client Uninstall Selection** page appears.

3. Select the client applications you want to uninstall and click **Uninstall**.
4. Click **Done** to close the uninstaller.

After the uninstallation is complete, the **Post-Uninstallation Summary** page appears, displaying the results of the uninstallation.

After you uninstall the Informatica clients, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica\_<Version>\_Client\_InstallLog.log file
- Informatica\_<Version>\_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

## Uninstalling Informatica Clients in Silent Mode

If you installed the Informatica clients in silent mode, uninstall the Informatica clients in silent mode.

### Creating the Properties File

Informatica provides a sample properties file that includes the properties required by the installer.

Customize the sample properties file to create a properties file and specify the options for your uninstallation. Then run the silent uninstallation.

1. Go to <Informatica installation directory>/Uninstaller\_Client.
2. Locate the sample SilentInput.properties file.
3. Create a backup copy of the SilentInput.properties file.
4. Use a text editor to open and modify the values of the properties file.

The following table describes the properties that you can modify:

Property Name	Description
DXT_COMP	Indicates whether to uninstall Informatica Developer. If the value is 1, the Developer tool will be uninstalled. If the value is 0, the Developer tool will not be uninstalled. Default is 1.

5. Save the SilentInput.properties file.

### Running the Silent Uninstaller

After you configure the properties file, run the silent uninstallation.

1. Go to <Informatica installation directory>/Uninstaller\_Client.
2. To run the silent installation, double-click the uninstaller.bat or uninstaller.exe file.

The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if you incorrectly configure the properties file or if the installation directory is not accessible.

After you uninstall the Informatica clients, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica\_<Version>\_Client\_InstallLog.log file
- Informatica\_<Version>\_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.



## APPENDIX A

# Starting and Stopping Informatica Services

This appendix includes the following topics:

- [Starting and Stopping Informatica Services Overview , 297](#)
- [Starting and Stopping the Informatica Services from the Console, 297](#)
- [Stopping Informatica in Informatica Administrator, 298](#)
- [Starting or Stopping Informatica from the Control Panel, 298](#)
- [Starting or Stopping Informatica from the Start Menu, 298](#)
- [Starting or Stopping Informatica from a Command Prompt, 299](#)
- [Rules and Guidelines for Starting or Stopping Informatica, 299](#)

## Starting and Stopping Informatica Services Overview

The Informatica service runs the Service Manager on the node. The Service Manager manages all domain functions and starts application services configured to run on the node. The method you use to start or stop Informatica depends on the operating system. You can use Informatica Administrator to shut down a node. When you shut down a node, you stop Informatica on the node.

The Informatica service also runs Informatica Administrator. You use Informatica Administrator to administer the Informatica domain objects and user accounts. Log in to Informatica Administrator to create the user accounts for users of Informatica and to create and configure the application services in the domain.

## Starting and Stopping the Informatica Services from the Console

Run `infaservice.sh` to start and stop the Informatica daemon. By default, `infaservice.sh` is installed in the following directory:

```
<Informatica installation directory>/tomcat/bin
```

1. Go to the directory where `infaservice.sh` is located.

2. At the command prompt, enter the following command to start the daemon:

```
infaservice.sh startup
```

Enter the following command to stop the daemon:

```
infaservice.sh shutdown
```

**Note:** If you use a softlink to specify the location of `infaservice.sh`, set the `INFA_HOME` environment variable to the location of the Informatica installation directory.

## Stopping Informatica in Informatica Administrator

When you shut down a node using Informatica Administrator, you stop the Informatica service on that node.

You can abort the processes that are running or allow them to complete before the service shuts down. If you shut down a node and abort the repository service processes running on the node, you can lose changes that have not yet been written to the repository. If you abort a node running integration service processes, the workflows will abort.

1. Log in to Informatica Administrator.
2. In the Navigator, select the node to shut down.
3. On the Domain tab **Actions** menu, select **Shutdown Node**.

## Starting or Stopping Informatica from the Control Panel

The procedure to start or stop the Informatica Windows service is the same as for all other Windows services.

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Right-click **Services** and select **Run as Administrator**.
4. Right-click the Informatica service.
5. If the service is running, click **Stop**.  
If the service is stopped, click **Start**.

## Starting or Stopping Informatica from the Start Menu

To start Informatica from the Windows Start menu, click **Programs > Informatica[Version] > Server**. Right-click **Start Informatica Services** and select **Run as Administrator**.

To stop Informatica from the Windows Start menu, click **Programs > Informatica[Version] > Server**. Right-click **Stop Informatica Services** and select **Run as Administrator**.

# Starting or Stopping Informatica from a Command Prompt

You can run `infaservice.bat` from the command line to start and stop the Informatica services on Windows.

By default, `infaservice.bat` is installed in the following directory:

```
<Informatica installation directory>\tomcat\bin
```

1. Open a command prompt as administrator.
2. Go to the directory where `infaservice.bat` is located.
3. Enter the following command to start the Informatica services:

```
infaservice.bat startup
```

Enter the following command to stop the Informatica services:

```
infaservice.bat shutdown
```

## Rules and Guidelines for Starting or Stopping Informatica

Consider the following rules and guidelines when starting and stopping Informatica on a node:

- When you shut down a node, the node is unavailable to the domain. If you shut down a gateway node and do not have another gateway node in the domain, the domain is unavailable.
- When you start Informatica, verify that the port used by the service on the node is available. For example, if you stop Informatica on a node, verify that the port is not used by any other process on the machine before you restart Informatica. If the port is not available, Informatica will fail to start.
- If you do not use Informatica Administrator to shut down a node, any process running on the node will be aborted. If you want to wait for all processes to complete before shutting down a node, use Informatica Administrator.
- If you have two nodes in a domain with one node configured as a primary node for an application service and the other node configured as a backup node, start Informatica on the primary node before you start the backup node. Otherwise, the application service will run on the backup node and not the primary node.

## APPENDIX B

# Managing Distribution Packages

This appendix includes the following topics:

- [Managing Distribution Packages Overview, 300](#)
- [Before You Begin, 300](#)
- [Install or Remove Distribution Packages in Console Mode, 301](#)
- [Install or Remove Distribution Packages in Silent Mode, 302](#)
- [After You Install, 302](#)

## Managing Distribution Packages Overview

You can use Integration Package Manager (the package manager) to install and remove distribution packages from the Informatica service and client machines.

A distribution package is a set of distribution binaries that you install within the domain for the following processing requirements:

- To push processing to the Hadoop or Databricks environment.
- To process complex files within the Informatica domain.
- To connect to the Hadoop or Databricks environment when you process within the Informatica domain.

You can install distribution packages if you didn't do so during the upgrade or install process or if you want to add a distribution package. You can remove a distribution package if you want to use a different package or if you installed a package that you don't use.

When you install or remove distribution packages, verify that you perform the operation on all service and client machines.

## Before You Begin

Before you run the package manager, perform tasks such as setting environment variables and downloading files.

1. Shut down the Informatica services.

2. Set one of the following environment variables:

Variable	Description
INFA_JDK_HOME	Location of the folder containing the supported Java Development Kit (JDK). Set the INFA_JDK_HOME environment variable in the following scenarios: <ul style="list-style-type: none"><li>- Informatica domain is on Windows or Linux</li><li>- Informatica client</li></ul>
INFA_JRE_HOME	Location of the folder containing the supported Java Runtime Environment (JRE). If the Informatica domain is on AIX, set the INFA_JRE_HOME environment variable.

3. Verify that the user that runs the package manager has read and write permissions on the Informatica installation directory and execute permissions on the executable file.
4. Download the following files from the Informatica Electronic Software Download site:
  - [Integration Package Manager](#)
  - [Distribution packages](#)
5. Extract the Integration Package Manager ZIP files to a local drive.
6. Copy the ZIP files of distribution packages that you need to the following location: <Integration Package Manager directory>/source  
**Note:** The package manager fails if the ZIP files for distribution packages aren't available in the source directory.

## Install or Remove Distribution Packages in Console Mode

You can run the package manager in console mode to install or remove distribution packages.

1. From the package manager directory, run one of the following commands:
  - `./Server.sh console` for Linux or UNIX
  - `Server.bat console` for Windows
  - `Client.bat console` for client**Note:** To run the command on Windows, use the administrator command prompt.
2. Enter the installation directory of the services or client and press **Enter**.
3. Choose the operation type and press **Enter**.
  - Select 1 to remove existing distribution packages.
  - Select 2 to install one or more distribution packages.The console lists the distribution packages that you can install or remove.
4. Enter the distribution packages that you want to install or remove, separating multiple packages with a comma, and press **Enter**.
5. Verify the installation or removal status in the package manager log file.  
You can find the log file in the following location: <Integration Package Manager directory>/IntegrationPackageManager\_<date and timestamp>.log

# Install or Remove Distribution Packages in Silent Mode

You can run the package manager in silent mode to install or remove distribution packages. The silent input properties file contains the properties for the package manager to run in silent mode for service and clients. Set the appropriate value for each property in the file.

1. Find the IntegrationPackageManager.properties file in the following location: `<Integration Package Manager directory>/`
2. Edit the properties file in a text editor.

The following table describes the properties that you can modify:

Property Name	Description
USER_INSTALL_DIR	The installation directory of the service or client.
OPERATION_TYPE	The operation that you want to perform: <ul style="list-style-type: none"><li>- Set to DELETE to remove existing distribution packages.</li><li>- Set to EXTRACT to install one or more distribution packages.</li></ul>
SELECTED_HADOOP_LIBRARIES	Lists the distribution packages and versions. Enter the distribution packages that you want to install or remove. Separate multiple packages with a comma.

3. Save the properties file.
4. From the package manager directory, run one of the following commands:
  - `./Server.sh silent` for Linux or UNIX
  - `Server.bat silent` for Windows
  - `Client.bat silent` for client

**Note:** To run the command on Windows, use the administrator command prompt.

5. Verify the installation or removal status in the package manager log file.

You can find the log file in the following location: `<Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log`

## After You Install

To use the distribution packages that are installed using the package manager, configure the property or environment variable in service and client machines.

### Configure the Developer Tool

After you install the distribution packages in the Developer tool, update the developerCore.ini file with the installed distribution package.

1. Find the developerCore.ini file in the following location: `<Informatica installation directory>\clients\DeveloperClient`

2. Edit the file to update the following property:

```
-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>
```

For example,

```
-DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1
```

3. Restart the Developer tool.

## Configure Environment Variables

Some adapters require environment variables for the Data Integration Service and Metadata Access Service to access the distribution packages. For more information, see

[Configure environment variables to process complex files.](#)

## APPENDIX C

# Connecting to Databases from UNIX or Linux

This appendix includes the following topics:

- [Connecting to Databases from UNIX or Linux Overview, 304](#)
- [Connecting to an IBM DB2 Universal Database, 305](#)
- [Connecting to an Informix Database, 307](#)
- [Connecting to a Microsoft SQL Server Database, 308](#)
- [Connecting to a Netezza Database, 309](#)
- [Connecting to an Oracle Database, 311](#)
- [Connecting to a PostgreSQL Database, 313](#)
- [Connecting to a Sybase ASE Database, 317](#)
- [Connecting to a Teradata Database, 319](#)
- [Connecting to a JDBC Data Source, 322](#)
- [Connecting to an ODBC Data Source, 322](#)
- [Sample odbc.ini File, 324](#)

## Connecting to Databases from UNIX or Linux Overview

To use native connectivity, you must install and configure the database client software for the database that you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To increase performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third party ODBC drivers that are Level 2 compliant or higher.

You must configure a database connection for the following services in the Informatica domain:

- PowerCenter Repository Service
- Model Repository Service



- Data Integration Service
- Analyst Service

When you connect to databases from Linux or UNIX, use native drivers to connect to IBM DB2, Oracle, or Sybase ASE databases. You can use ODBC to connect to other sources and targets.

## Connecting to an IBM DB2 Universal Database

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

### Configuring Native Connectivity

You can configure native connectivity to an IBM DB2 database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. To configure connectivity on the machine where the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process runs, log in to the machine as a user who can start a service process.
2. Set the DB2INSTANCE, INSTHOME, DB2DIR, and PATH environment variables.

The UNIX IBM DB2 software always has an associated user login, often db2admin, which serves as a holder for database configurations. This user holds the instance for DB2.

**DB2INSTANCE.** The name of the instance holder.

Using a Bourne shell:

```
$ DB2INSTANCE=db2admin; export DB2INSTANCE
```

Using a C shell:

```
$ setenv DB2INSTANCE db2admin
```

**INSTHOME.** This is db2admin home directory path.

Using a Bourne shell:

```
$ INSTHOME=~db2admin
```

Using a C shell:

```
$ setenv INSTHOME ~db2admin>
```

**DB2DIR.** Set the variable to point to the IBM DB2 CAE installation directory. For example, if the client is installed in the /opt/IBM/db2/V9.7 directory:

Using a Bourne shell:

```
$ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
```

Using a C shell:

```
$ setenv DB2DIR /opt/IBM/db2/V9.7
```

**PATH.** To run the IBM DB2 command line programs, set the variable to include the DB2 bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:${DB2DIR}/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:$DB2DIR/bin
```

3. Set the shared library variable to include the DB2 lib directory.

The IBM DB2 client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

The shared library path must also include the Informatica installation directory (*server\_dir*).

Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

Operating System	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export  
LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
```

For AIX:

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again or run the source command.

Using a Bourne shell:

```
$ source .profile
```

Using a C shell:

```
$ source .cshrc
```

5. If the DB2 database resides on the same machine on which the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process runs, configure the DB2 instance as a remote instance.

Run the following command to verify if there is a remote entry for the database:

```
DB2 LIST DATABASE DIRECTORY
```

The command lists all the databases that the DB2 client can access and their configuration properties. If this command lists an entry for "Directory entry type" of "Remote," skip to [7](#).

6. If the database is not configured as remote, run the following command to verify whether a TCP/IP node is cataloged for the host:

```
DB2 LIST NODE DIRECTORY
```

If the node name is empty, you can create one when you set up a remote database. Use the following command to set up a remote database and, if needed, create a node:

```
db2 CATALOG TCPIP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

Run the following command to catalog the database:

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

For more information about these commands, see the database documentation.

7. Verify that you can connect to the DB2 database. Run the DB2 Command Line Processor and run the command:

```
CONNECT TO <dbalias> USER <username> USING <password>
```

If the connection is successful, clean up with the `CONNECT RESET` or `TERMINATE` command.

## Connecting to an Informix Database

Use ODBC to connect to an Informix database on UNIX or Linux.

### Configuring ODBC Connectivity

You can configure ODBC connectivity to an Informix database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Set the `ODBCHOME` environment variable to the ODBC installation directory. For example:

Using a Bourne shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Using a C shell:

```
$ setenv ODBCHOME <Informatica server home>/ODBC7.1
```

2. Set the `ODBCINI` environment variable to the location of the `odbc.ini` file. For example, if the `odbc.ini` file is in the `$ODBCHOME` directory:

Using a Bourne shell:

```
ODBCINI=$ODBCHOME/odbc.ini; export ODBCINI
```

Using a C shell:

```
$ setenv ODBCINI $ODBCHOME/odbc.ini
```

3. Edit the existing `odbc.ini` file in the `$ODBCHOME` directory or copy this `odbc.ini` file to the UNIX home directory and edit it.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

4. Add an entry for the Informix data source under the section [ODBC Data Sources] and configure the data source. For example:

```
[Informix Wire Protocol]
Driver=/export/home/Informatica/10.0.0/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
```

```

HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1

```

5. Set the PATH and shared library environment variables by executing the script `odbc.sh` or `odbc.csh` in the `$ODBCHOME` directory.

Using a Bourne shell:

```
sh odbc.sh
```

Using a C shell:

```
source odbc.csh
```

6. Verify that you can connect to the Informix database using the ODBC data source. If the connection fails, see the database documentation.

## Connecting to a Microsoft SQL Server Database

Use the Microsoft SQL Server connection to connect to a Microsoft SQL Server database from a UNIX or Linux machine.

### Configuring SSL Authentication through ODBC

You can configure SSL authentication for Microsoft SQL Server through ODBC using the DataDirect New SQL Server Wire Protocol driver.

1. Open the `odbc.ini` file and add an entry for the ODBC data source and DataDirect New SQL Server Wire Protocol driver under the section `[ODBC Data Sources]`.
2. Add the attributes in the `odbc.ini` file for configuring SSL.

The following table lists the attributes that you must add to the `odbc.ini` file when you configure SSL authentication:

Attribute	Description
EncryptionMethod	The method that the driver uses to encrypt the data sent between the driver and the database server. Set the value to 1 to encrypt data using SSL.
ValidateServerCertificate	Determines whether the driver validates the certificate sent by the database server when SSL encryption is enabled. Set the value to 1 for the driver to validate the server certificate.
TrustStore	The location and name of the trust store file. The trust store file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication.

Attribute	Description
TrustStorePassword	The password to access the contents of the trust store file.
HostNameInCertificate	Optional. The host name that is established by the SSL administrator for the driver to validate the host name contained in the certificate.

## Configuring Custom Properties for Microsoft SQL Server

You can configure custom properties for Microsoft SQL Server to improve bulk load performance.

1. Launch the PowerCenter client and connect to Workflow Manager.
2. Open a workflow and select a session that you want to configure.
3. Click the **Config Object** tab.
4. Change the value of the **Default Buffer Block** size to 5 MB. You can also use the following command:  
`$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>`  
 To get optimum throughput for a row size of 1 KB, you must set the Buffer Block size to 5 MB.
5. Click the **Properties** tab.
6. Change the **Commit Interval** to 100000 if the session contains a relational target.
7. Set the **DTM Buffer Size**. The optimum DTM Buffer Size is ((10 x Block Buffer size) x number of partitions).

## Connecting to a Netezza Database

Install and configure Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the DataDirect Driver Manager in the DataDirect driver package shipped with the Informatica product to configure the Netezza data source details in the odbc.ini file.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a Netezza database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the ODBCHOME, NZ\_ODBC\_INI\_PATH, and PATH environment variables.

**ODBCHOME.** Set the variable to the ODBC installation directory. For example:

Using a Bourne shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Using a C shell:

```
$ setenv ODBCHOME =<Informatica server home>/ODBC7.1
```

**PATH.** Set the variable to the ODBC\_HOME/bin directory. For example:

Using a Bourne shell:

```
PATH="${PATH}:%ODBC_HOME/bin"
```

Using a C shell:

```
% setenv PATH ${PATH}:%ODBC_HOME/bin
```

**NZ\_ODBC\_INI\_PATH.** Set the variable to point to the directory that contains the odbc.ini file. For example, if the odbc.ini file is in the \$ODBC\_HOME directory:

Using a Bourne shell:

```
NZ_ODBC_INI_PATH=$ODBC_HOME; export NZ_ODBC_INI_PATH
```

Using a C shell:

```
% setenv NZ_ODBC_INI_PATH $ODBC_HOME
```

3. Set the shared library environment variable.

The shared library path must contain the ODBC libraries. It must also include the Informatica services installation directory (server\_dir).

Set the shared library environment variable based on the operating system. Set the Netezza library folder to <NetezzaInstallationDir>/lib64.

The following table describes the shared library variables for each operating system:

Operating System	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
% LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBC_HOME/  
lib:<NetezzaInstallationDir>/lib64"  
export LD_LIBRARY_PATH
```

- Using a C shell:

```
% setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBC_HOME/  
lib:<NetezzaInstallationDir>/lib64"
```

For AIX

- Using a Bourne shell:

```
% LIBPATH=${LIBPATH}:%HOME/server_dir:%ODBC_HOME/lib:<NetezzaInstallationDir>/  
lib64; export LIBPATH
```

- Using a C shell:

```
% setenv LIBPATH ${LIBPATH}:%HOME/server_dir:%ODBC_HOME/  
lib:<NetezzaInstallationDir>/lib64
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

This file exists in \$ODBC\_HOME directory.

```
% cp $ODBC_HOME/odbc.ini $HOME/.odbc.ini
```

Add an entry for the Netezza data source under the section [ODBC Data Sources] and configure the data source.

For example:

```
[NZSQL]
Driver = /export/home/appsga/thirdparty/netezza/lib64/libnzodbc.so
Description = NetezzaSQL ODBC
Servername = netezza1.informatica.com
Port = 5480
Database = infa
Username = admin
Password = password
Debuglogging = true
StripCRLF = false
PreFetch = 256
Protocol = 7.0
ReadOnly = false
ShowSystemTables = false
Socket = 16384
DateFormat = 1
TranslationDLL =
TranslationName =
TranslationOption =
NumericAsChar = false
```

For more information about Netezza connectivity, see the Netezza ODBC driver documentation.

5. Verify that the last entry in the `odbc.ini` file is `InstallDir` and set it to the ODBC installation directory.

For example:

```
InstallDir=<Informatica install directory>/<ODBCHOME directory>
```

6. Edit the `.cshrc` or `.profile` file to include the complete set of shell commands.
7. Restart the Informatica services.

## Connecting to an Oracle Database

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

## Configuring Native Connectivity

You can configure native connectivity to an Oracle database to increase performance.

The following steps provide a guideline for configuring native connectivity through Oracle Net Services or Net8. For specific instructions, see the database documentation.

1. To configure connectivity for the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. Set the `ORACLE_HOME`, `NLS_LANG`, `TNS_ADMIN`, and `PATH` environment variables.

**ORACLE\_HOME.** Set the variable to the Oracle client installation directory. For example, if the client is installed in the `/HOME2/oracle` directory, set the variable as follows:

Using a Bourne shell:

```
$ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
```

Using a C shell:

```
$ setenv ORACLE_HOME /HOME2/oracle
```

**NLS\_LANG.** Set the variable to the locale (language, territory, and character set) you want the database client and server to use with the login. The value of this variable depends on the configuration. For example, if the value is `american_america.UTF8`, set the variable as follows:

Using a Bourne shell:

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

Using a C shell:

```
$ NLS_LANG american_america.UTF8
```

To determine the value of this variable, contact the administrator.

**ORA\_SDTZ.** To set the default session time zone when the Data Integration Service reads or writes the Timestamp with Local Time Zone data, specify the `ORA_SDTZ` environment variable.

You can set the `ORA_SDTZ` environment variable to any of the following values:

- Operating system local time zone ('OS\_TZ')
- Database time zone ('DB\_TZ')
- Absolute offset from UTC (for example, '-05:00')
- Time zone region name (for example, 'America/Los\_Angeles')

You can set the environment variable at the machine where Informatica server runs.

**TNS\_ADMIN.** If the `tnsnames.ora` file is not in the same location as the Oracle client installation location, set the `TNS_ADMIN` environment variable to the directory where the `tnsnames.ora` file resides. For example, if the file is in the `/HOME2/oracle/files` directory, set the variable as follows:

Using a Bourne shell:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Using a C shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

**Note:** By default, the `tnsnames.ora` file is stored in the following directory: `$ORACLE_HOME/network/admin`.

**PATH.** To run the Oracle command line programs, set the variable to include the Oracle bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

### 3. Set the shared library environment variable.

The Oracle client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

The shared library path must also include the Informatica installation directory (`server_dir`).

Set the shared library environment variable to `LD_LIBRARY_PATH`.

For example, use the following syntax:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
```



- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:%HOME/server_dir:%ORACLE_HOME/lib
```

4. Edit the `.cshrc` or `.profile` to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

Using a Bourne shell:

```
$ source .profile
```

Using a C shell:

```
$ source .cshrc
```

5. Verify that the Oracle client is configured to access the database.

Use the SQL\*Net Easy Configuration Utility or copy an existing `tnsnames.ora` file to the home directory and modify it.

The `tnsnames.ora` file is stored in the following directory: `%ORACLE_HOME/network/admin`.

Enter the correct syntax for the Oracle connect string, typically `databasename.world`.

Here is a sample `tnsnames.ora` file. Enter the information for the database.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
          (PROTOCOL = TCP)
          (Host = mymachine)
          (Port = 1521)
        )
      )
    )
  (CONNECT_DATA =
    (SID = MYORA7)
    (GLOBAL_NAMES = mydatabase.world)
```

Here is a sample `tnsnames.ora` file to connect to Oracle using Oracle Connection Manager:

```
ORCL19C_CMAN =
  (description=
    (address_list=
      (source_route=yes)
      (address=(protocol=tcp) (host=lnrh74ocm.mycompany.com) (port=1521))
      (address=(protocol=tcp) (host=lnrh74oradb.mycompany.com) (port=1521))
    )
    (connect_data=
      (service_name=ORCL19C.mycompany.com)
    )
  )
```

6. Verify that you can connect to the Oracle database.

To connect to the Oracle database, launch SQL\*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

Enter the user name and connect string as defined in the `tnsnames.ora` file.

## Connecting to a PostgreSQL Database

For native connectivity, install the version of PostgreSQL client appropriate for the PostgreSQL database server version.

To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the PostgreSQL client and PostgreSQL database server. You must also install the same version of the PostgreSQL client on all machines that require it. To verify compatibility, contact PostgreSQL.

## Configuring Native Connectivity

You can configure native connectivity to a PostgreSQL database to increase performance.

The following steps provide a guideline for configuring native connectivity through PostgreSQL. For specific instructions, see the database documentation.

1. To configure connectivity for the PowerCenter Integration Service and PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. To configure a PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the `pg_service.conf` file in the following format:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter repository database service name
```

Ensure that the entries for the `[PCRS_DB_SERVICE_NAME]` match the configuration for the PowerCenter Repository Service. In the `pg_service.conf` file, you can securely connect to PostgreSQL for the PowerCenter repository. To set the secure connect, set the security property and the required database properties in the `pg_service.conf` file in the following format: `sslmode=require`

3. Set the `PGSERVICEFILE`, `PGHOME`, and `PATH` environment variables.

**PGSERVICEFILE.** Set the variable to the `pg_service.conf` file that contains the connection parameters for PostgreSQL database connection. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Using a C shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file
directory>/pg_service.conf
```

**PGHOME.** Set the variable to the PostgreSQL installation path where you have installed the PostgreSQL client. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

Using a C shell:

```
$ setenv PGHOME /usr/pgsql-10
```

**PATH.** To run the PostgreSQL command line programs, set the variable to include the PostgreSQL client directory, `psql`. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

Using a C shell:

```
$ setenv PATH ${PGHOME}:${PATH}
```

4. Set the shared library environment variable.

The PostgreSQL client software contains a number of shared library components that the PowerCenter Integration Service and PowerCenter Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

The shared library path must also include the Informatica installation directory (`server_dir`).

Set the shared library environment variable to LD\_LIBRARY\_PATH.

For example, use the following syntax:

- Using a Bourne shell:

```
$ export LD_LIBRARY_PATH; LD_LIBRARY_PATH $PGHOME/lib
$ LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH $PGHOME/lib
$ setenv LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

5. Verify that you can connect to the PostgreSQL database.

To connect to the PostgreSQL database, launch the psql utility and enter the connectivity information.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a PostgreSQL database on UNIX or Linux.

You can configure connectivity to PostgreSQL through ODBC using the DataDirect PostgreSQL Wire Protocol driver.

Review the following tasks for a guideline for configuring ODBC connectivity to PostgreSQL:

1. Set the environment variable for PostgreSQL
2. Configure ODBC connectivity in the ODBC.ini file
3. Update the PowerCenter repository with the PostgreSQL data source name
4. Verify the PostgreSQL connection with the ODBC data source

For specific instructions, see the database documentation.

### Step 1. Set the Environment Variable

1. In the Administrator tool, click **Manage > Services and Nodes**.
2. In the Domain Navigator, select the PowerCenter Repository Service.
3. In the contents panel, click the Processes view. In the Environment Variables section, set the variable name as POSTGRES\_ODBC and the value to 1.

### Step 2. Configure ODBC Connectivity

1. Set the ODBCHOME environment variable to the ODBC installation directory. For example:

Using a Bourne shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Using a C shell:

```
$ setenv ODBCHOME <Informatica server home>/ODBC7.1
```

2. Edit the existing odbc.ini file in the \$ODBCHOME directory or copy the odbc.ini file to the UNIX home directory and edit it.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

3. Open the odbc.ini file and add a entry for DataDirect PostgreSQL Wire Protocol data sources.

Configure the data source name, driver path, host name, and port number to connect to the PostgreSQL database. For example:

```
[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBufLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10
```

#### 4. Set the PATH environment variable.

Using a Bourne shell:

```
$ PATH=${PATH}:%ODBCHOME/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:%ODBCHOME/bin
```

#### 5. Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

For example, use the following syntax to set the LD\_LIBRARY\_PATH for Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:%HOME/server_dir :%ODBCHOME/lib; export
LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH %HOME/server_dir:%ODBCHOME/lib:%LD_LIBRARY_PATH
```

For example, use the following syntax to set the LIBPATH for AIX:

- Using a Bourne shell:  

```
$ LIBPATH=${LIBPATH}:%HOME/server_dir :%ODBCHOME/lib; export LIBPATH
```
- Using a C shell:  

```
$ setenv LIBPATH ${LIBPATH}:%HOME/server_dir :%ODBCHOME/lib
```

### Step 3. Update the PowerCenter Repository Database Properties

1. Select the PowerCenter Repository Service in the Administrator tool.
2. In the database properties section, enter the same data source name that you specified for PostgreSQL in the ODBC.ini file.
3. Save your changes.

### Step 4. Verify PostgreSQL Connection

1. Verify that you can connect to the PostgreSQL database using the ODBC data source.
2. If the connection fails, see the database documentation.

## Connecting to a Sybase ASE Database

For native connectivity, install the version of Open Client appropriate for your database version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

## Configuring Native Connectivity

You can configure native connectivity to a Sybase ASE database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. To configure connectivity to the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. Set the SYBASE and PATH environment variables.

**SYBASE.** Set the variable to the Sybase Open Client installation directory. For example if the client is installed in the /usr/sybase directory:

Using a Bourne shell:

```
$ SYBASE=/usr/sybase; export SYBASE
```

Using a C shell:

```
$ setenv SYBASE /usr/sybase
```

**PATH.** To run the Sybase command line programs, set the variable to include the Sybase OCS bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
```

3. Set the shared library environment variable.

The Sybase Open Client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

The shared library path must also include the installation directory of the Informatica services (*server\_dir*).

Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system.

Operating System	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

Using a Bourne shell:

```
$ source .profile
```

Using a C shell:

```
$ source .cshrc
```

5. Verify the Sybase ASE server name in the Sybase interfaces file stored in the \$SYBASE directory.

6. Optionally, to connect to the SSL-enabled Sybase ASE database, perform the following tasks:
- Specify the following security attributes on the **Security** tab when you configure the data source name in the Sybase driver property:

Attribute	Description
Encryption Method	Indicates whether data is encrypted when transmitted over the network. Select SSL.
Validate Server Certificate	Indicates whether Informatica validates the certificate that is sent by the database server when SSL encryption is enabled.
Trust Store	The location and name of the trust store file.
Trust Store Password	The password to access the contents of the trust store file.
Host Name In Certificate	The host name that is established by the SSL administrator to validate the host name contained in the certificate.

- Add the Sybase ASE server certificate to the trusted.txt file in the Sybase ASE client.
- Add the following Sybase ASE server connection details to the Sybase interface file:

```
<server_instance_name>  
  master tcp ether <host name> <port number> ssl="CN='common_name'"  
  query tcp ether <host name> <port number> ssl="CN='common_name'"
```

7. Verify that you can connect to the Sybase ASE database.

To connect to the Sybase ASE database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

User names and database names are case sensitive.

## Connecting to a Teradata Database

Install and configure native client software on the machines where the Data Integration Service or PowerCenter Integration Service process runs. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the Data Integration Service or PowerCenter Integration Service runs. You must also configure ODBC connectivity.

**Note:** Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a Teradata database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the `TERADATA_HOME`, `ODBCHOME`, and `PATH` environment variables.

**TERADATA\_HOME.** Set the variable to the Teradata driver installation directory. The defaults are as follows:

Using a Bourne shell:

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

Using a C shell:

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

**ODBCHOME.** Set the variable to the ODBC installation directory. For example:

Using a Bourne shell:

```
$ ODBCHOME=$INFA_HOME/ODBC<version>; export ODBCHOME
```

Using a C shell:

```
$ setenv ODBCHOME $INFA_HOME/ODBC<version>
```

**PATH.** To run the `ddtestlib` utility, to verify that the DataDirect ODBC driver manager can load the driver files, set the variable as follows:

Using a Bourne shell:

```
PATH="${PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin"
```

Using a C shell:

```
$ setenv PATH ${PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin
```

3. Set the shared library environment variable.

The Teradata software contains multiple shared library components that the integration service process loads dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

The shared library path must also include installation directory of the Informatica service (*server\_dir*).

Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

Operating System	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBCHOME/lib:
%TERADATA_HOME/lib64:%TERADATA_HOME/odbc_64/lib";
export LD_LIBRARY_PATH
```



- Using a C shell:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBCHOME/
lib:%TERADATA_HOME/lib64:

$TERADATA_HOME/odbc_64/lib"
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:%HOME/server_dir:%ODBCHOME/lib:%TERADATA_HOME/
lib64:%TERADATA_HOME/odbc_64/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:%HOME/server_dir:%ODBCHOME/lib:%TERADATA_HOME/lib64:

$TERADATA_HOME/odbc_64/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

This file exists in %ODBCHOME directory.

```
$ cp %ODBCHOME/odbc.ini %HOME/.odbc.ini
```

Add an entry for the Teradata data source under the section [ODBC Data Sources] and configure the data source.

For example, for Teradata Parallel Transporter utilities, version 15.10:

```
MY_TERADATA_SOURCE=Teradata Driver
[MY_TERADATA_SOURCE]
Driver=/opt/teradata/client/15.10/lib64/tdata.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=208.199.59.208
DateTimeFormat=AAA
SessionMode=ANSI
DefaultDatabase=
Username=
Password=
```

For example, for Teradata Parallel Transporter utilities, version 16.20:

```
MY_TERADATA_SOURCE=Teradata Driver
[dwtera]
Driver=/opt/teradata/client/16.20/lib64/tdataodbc_sb64.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=tdvbel510
LastUser=
Username=
Password=
Database=
DefaultDatabase=
UseNativeLOBSupport=Yes
CharacterSet=UTF8
SessionMode=ANSI
```

5. Set the DateTimeFormat to AAA in the Teradata data ODBC configuration.
6. Optionally, set the SessionMode to ANSI. When you use ANSI session mode, Teradata does not roll back the transaction when it encounters a row error.

If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the integration service process cannot detect the rollback, and does not report this in the session log.

7. To configure connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC DSN, leave the DefaultDatabase field empty.

For more information about Teradata connectivity, see the Teradata ODBC driver documentation.

8. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

For example:

```
InstallDir=<Informatica installation directory>/ODBC<version>
```

9. Edit the .cshrc or .profile to include the complete set of shell commands.
10. Save the file and either log out and log in again, or run the source command.

Using a Bourne shell:

```
$ source .profile
```

Using a C shell:

```
$ source .cshrc
```

11. For each data source you use, make a note of the file name under the Driver=<parameter> in the data source entry in odbc.ini. Use the *ddtestlib* utility to verify that the DataDirect ODBC driver manager can load the driver file.

For example, if you have the driver entry:

```
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

run the following command:

```
ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

12. Test the connection using BTEQ or another Teradata client tool.

## Connecting to a JDBC Data Source

To enable the the Data Integration Service to write to relational targets, download JDBC driver .jar files to the Data Integration Service host and to all client machines that run mappings that have relational targets.

Obtain the driver .jar file from the database vendor. For example, to access an Oracle database, download the file *ojdbc.jar* from the Oracle website.

1. Place the JDBC driver .jar file in the following directory on the Data Integration Service machine <Informatica installation directory>/externaljdbcjars. Then recycle the Data Integration Service.
2. Place the JDBC driver .jar file in the following directory on machines that host the Developer tool: <Informatica installation directory>/clients/externaljdbcjars. Then recycle the Developer tool.

## Connecting to an ODBC Data Source

Install and configure native client software on the machine where the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service run. Also install and configure any underlying client access software required by the ODBC driver. To ensure compatibility between Informatica and the databases, use the appropriate database client libraries.

The Informatica installation includes DataDirect ODBC drivers. If the odbc.ini file contains connections that use earlier versions of the ODBC driver, update the connection information to use the new drivers. Use the System DSN to specify an ODBC data source on Windows.

1. On the machine where the application service runs, log in as a user who can start a service process.

2. Set the ODBC7HOME and PATH environment variables.

**ODBC7HOME.** Set to the DataDirect ODBC installation directory. For example, if the install directory is /export/home/Informatica/10.0.0/ODBC7.1.

Using a Bourne shell:

```
$ ODBC7HOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBC7HOME
```

Using a C shell:

```
$ setenv ODBC7HOME /export/home/Informatica/10.0.0/ODBC7.1
```

**PATH.** To run the ODBC command line programs, like *ddtestlib*, set the variable to include the odbc bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:${ODBC7HOME}/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:${ODBC7HOME}/bin
```

Run the *ddtestlib* utility to verify that the DataDirect ODBC driver manager can load the driver files.

3. Set the shared library environment variable.

The ODBC software contains a number of shared library components that the service processes load dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

The shared library path must also include the Informatica installation directory (*server\_dir*).

Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

Operating System	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:${HOME}/server_dir:$ODBC7HOME/lib; export LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBC7HOME:${LD_LIBRARY_PATH}
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$ODBC7HOME/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$ODBC7HOME/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

This file exists in \$ODBC7HOME directory.

```
$ cp $ODBC7HOME/odbc.ini $HOME/.odbc.ini
```

Add an entry for the ODBC data source under the section [ODBC Data Sources] and configure the data source.

For example:

```
MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
[MY_MSSQLSERVER_ODBC_SOURCE]
Driver=<path to ODBC drivers>
Description=DataDirect 8.0 SQL Server Wire Protocol
Database=<SQLServer_database_name>
LogonID=<username>
Password=<password>
Address=<TCP/IP address>,<port number>
QuoteId=No
AnsiNPW=No
ApplicationsUsingThreads=1
```

This file might already exist if you have configured one or more ODBC data sources.

5. Verify that the last entry in the `odbc.ini` is `InstallDir` and set it to the `odbc` installation directory.

For example:

```
InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
```

6. If you use the `odbc.ini` file in the home directory, set the `ODBCINI` environment variable.

Using a Bourne shell:

```
$ ODBCINI=/HOME/.odbc.ini; export ODBCINI
```

Using a C shell:

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. Edit the `.cshrc` or `.profile` to include the complete set of shell commands. Save the file and either log out and log in again, or run the `source` command.

Using a Bourne shell:

```
$ source .profile
```

Using a C shell:

```
$ source .cshrc
```

8. Use the `ddtestlib` utility to verify that the DataDirect ODBC driver manager can load the driver file you specified for the data source in the `odbc.ini` file.

For example, if you have the driver entry:

```
Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

run the following command:

```
ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

9. Install and configure any underlying client access software needed by the ODBC driver.

**Note:** While some ODBC drivers are self-contained and have all information inside the `.odbc.ini` file, most are not. For example, if you want to use an ODBC driver to access Sybase IQ, you must install the Sybase IQ network client software and set the appropriate environment variables.

To use the Informatica ODBC drivers (`DWxxxxnn.so`), manually set the `PATH` and shared library path environment variables. Alternatively, run the `odbc.sh` or `odbc.csh` script in the `$ODBCHOME` folder. This script will set the required `PATH` and shared library path environment variables for the ODBC drivers provided by Informatica.

## Sample odbc.ini File

The following sample shows the entries for the ODBC drivers in the `ODBC.ini` file:

```
[ODBC Data Sources]
SQL Server Legacy Wire Protocol=DataDirect 7.1 SQL Server Legacy Wire Protocol
```

```

DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 8.0 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 8.0 SQL Server Wire Protocol
MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/"Informatica installation directory"/ODBC7.1
Trace=0
TraceFile=odbctrace.out
TraceDll=/"Informatica installation directory"/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=/"Informatica installation directory"/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0

```

```

ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora28.so
Description=DataDirect 8.0 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0

```

```

FailoverPreconnect=0
FetchTSWTZasTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
ProcedureRetResults=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0

```

```

LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNFW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so

```



```

Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>

```

```

QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10

```

**Note:** You might have to customize the DSN entries in the `ODBC.ini` file based on the third-party driver that you use. For more information about the DSN entries, see the corresponding third-party driver documentation.

## APPENDIX D

# Connecting to Databases from Windows

This appendix includes the following topics:

- [Connecting to Databases from Windows Overview, 331](#)
- [Connecting to an IBM DB2 Universal Database from Windows, 332](#)
- [Connecting to an Informix Database from Windows, 332](#)
- [Connecting to Microsoft Access and Microsoft Excel from Windows, 333](#)
- [Connecting to a Microsoft SQL Server Database from Windows, 333](#)
- [Connecting to a Netezza Database from Windows, 335](#)
- [Connecting to an Oracle Database from Windows, 336](#)
- [Connecting to a PostgreSQL Database, 337](#)
- [Connecting to a Sybase ASE Database from Windows, 339](#)
- [Connecting to a Teradata Database from Windows, 340](#)

## Connecting to Databases from Windows Overview

Configure connectivity to enable communication between clients, services, and other components in the domain.

To use native connectivity, you must install and configure the database client software for the database that you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To increase performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third party ODBC drivers that are Level 2 compliant or higher.

The Informatica installation includes DataDirect JDBC drivers. You can use these drivers without performing additional steps. You can also download JDBC Type 4 drivers from third-party vendors to connect to sources and targets. You can use any third-party JDBC driver that is JDBC 3.0 or later.

You must configure a database connection for the following services in the Informatica domain:

- PowerCenter Repository Service

- Model Repository Service
- Data Integration Service
- Analyst Service

## Connecting to an IBM DB2 Universal Database from Windows

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

### Configuring Native Connectivity

You can configure native connectivity to an IBM DB2 database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. Verify that the following environment variable settings have been established by IBM DB2 Client Application Enabler (CAE):
 

```
DB2HOME=C:\IBM\SQLLIB
DB2INSTANCE=DB2
DB2CODEPAGE=1208 (Sometimes required. Use only if you encounter problems. Depends on the locale, you may use other values.)
```
2. Verify that the PATH environment variable includes the IBM DB2 bin directory. For example:
 

```
PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
```
3. Configure the IBM DB2 client to connect to the database that you want to access. To configure the IBM DB2 client:
  - a. Launch the IBM DB2 Configuration Assistant.
  - b. Add the database connection.
  - c. Bind the connection.
4. Run the following command in the IBM DB2 Command Line Processor to verify that you can connect to the IBM DB2 database:
 

```
CONNECT TO <dbalias> USER <username> USING <password>
```
5. If the connection is successful, run the TERMINATE command to disconnect from the database. If the connection fails, see the database documentation.

## Connecting to an Informix Database from Windows

Use ODBC to connect to an Informix database on Windows. Create an ODBC data source by using the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

**Note:** If you use the DataDirect ODBC driver provided by Informatica, you do not need the database client. The ODBC wire protocols do not require the database client software to connect to the database.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to an Informix database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source using the DataDirect ODBC Wire Protocol driver for Informix provided by Informatica.
2. Verify that you can connect to the Informix database using the ODBC data source.

## Connecting to Microsoft Access and Microsoft Excel from Windows

Configure connectivity to the Informatica components on Windows.

Install Microsoft Access or Excel on the machine where the Data Integration Service and PowerCenter Integration Service processes run. Create an ODBC data source for the Microsoft Access or Excel data you want to access.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a Microsoft Access or Excel database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source using the driver provided by Microsoft.
2. To avoid using empty string or nulls, use the reserved words PmNullUser for the user name and PmNullPasswd for the password when you create a database connection.

## Connecting to a Microsoft SQL Server Database from Windows

You can connect to a Microsoft SQL Server database through the ODBC or the OLEDB provider type.

## Configuring Native Connectivity

You can configure native connectivity to the Microsoft SQL Server database by using the ODBC (default) or OLEDB provider types.

If you choose the ODBC provider type, you can enable the Use DSN option to use the DSN configured in the Microsoft ODBC Administrator as the connect string. If you do not enable the Use DSN option, you must specify the server name and database name in the connection properties.

If you choose the OLEDB provider type, you must install the Microsoft SQL Server 2012 Native Client to configure native connectivity to the Microsoft SQL Server database. If you cannot connect to the database, verify that you correctly entered all of the connectivity information.

You can download the Microsoft SQL Server 2012 Native Client from the following Microsoft website:  
<http://www.microsoft.com/en-in/download/details.aspx?id=29065>.

After you upgrade, the Microsoft SQL Server connection is set to the OLEDB provider type by default. It is recommended that you upgrade all your Microsoft SQL Server connections to use the ODBC provider type. You can upgrade all your Microsoft SQL Server connections to the ODBC provider type by using the following commands:

- If you are using PowerCenter, run the following command: `pmrep upgradeSqlServerConnection`
- If you are using the Informatica platform, run the following command: `infacmd.sh isp upgradeSQLSConnection`

For specific connectivity instructions, see the database documentation.

## Rules and Guidelines for Microsoft SQL Server

Consider the following rules and guidelines when you configure ODBC connectivity to a Microsoft SQL Server database on Windows:

- If you want to use a Microsoft SQL Server connection without using a Data Source Name (DSN less connection), you must configure the `odbcinst.ini` environment variable.
- If you are using a DSN connection, you must add the entry "EnableQuotedIdentifiers=1" to the ODBC DSN. If you do not add the entry, data preview and mapping run fail.
- When you use a DSN connection, you can configure the DataDirect specific properties. For more information about how to configure and use the Data Direct specific properties, see the DataDirect documentation.
- You can use the Microsoft SQL Server NTLM authentication on a DSN less Microsoft SQL Server connection on the Microsoft Windows platform.
- If the Microsoft SQL Server table contains a UUID data type and if you are reading data from an SQL table and writing data to a flat file, the data format might not be consistent between the OLE DB and ODBC connection types.
- You cannot use SSL connection on a DSN less connection. If you want to use SSL, you must use the DSN connection. Enable the Use DSN option and configure the SSL options in the `odbc.ini` file.
- If the Microsoft SQL Server uses Kerberos authentication, you must set the `GSSClient` property to point to the Informatica Kerberos libraries. Use the following path and filename: `<Informatica installation directory>/server/bin/libgssapi_krb5.so.2`. Create an entry for the `GSSClient` property in the DSN entries section in `odbc.ini` for a DSN connection or in the SQL Server wire protocol section in `odbcinst.ini` for a connection that does not use DSN.
- If you use the DataDirect ODBC driver to connect to Microsoft SQL Server, the Decimal data rounds off within the target database based on the scale values in the database tables. For example, if the scale is 5, the target Decimal data round-off occurs after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 rounds off to a target Decimal value of 12.34568.
- If you use Microsoft SQL Server Native client to configure native connectivity to Microsoft SQL Server databases, the Decimal data truncates based on the specified scale in the target database tables. For example, if the scale is 5, the Decimal data truncation occurs after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 truncates to a target Decimal value of 12.34567.

## Configuring Custom Properties for Microsoft SQL Server

You can configure custom properties for Microsoft SQL Server to improve bulk load performance.

1. Launch the PowerCenter client and connect to Workflow Manager.
2. Open a workflow and select a session that you want to configure.
3. Click the **Config Object** tab.
4. Change the value of the **Default Buffer Block** size to 5 MB. You can also use the following command:  

```
$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>
```

To get optimum throughput for a row size of 1 KB, you must set the Buffer Block size to 5 MB.
5. Click the **Properties** tab.
6. Change the **Commit Interval** to 100000 if the session contains a relational target.
7. Set the **DTM Buffer Size**. The optimum DTM Buffer Size is ((10 x Block Buffer size) x number of partitions).

## Connecting to a Netezza Database from Windows

Install and configure ODBC on the machines where the PowerCenter Integration Service process runs and where you install the PowerCenter Client. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity.
- **PowerCenter Client.** Install the Netezza ODBC driver on each PowerCenter Client machine that accesses the Netezza database. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity. Use the Workflow Manager to create a database connection object for the Netezza database.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a Netezza database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source for each Netezza database that you want to access.  

To create the ODBC data source, use the driver provided by Netezza.

Create a System DSN if you start the Informatica service with a Local System account logon. Create a User DSN if you select the This account log in option to start the Informatica service.

After you create the data source, configure the properties of the data source.
2. Enter a name for the new ODBC data source.
3. Enter the IP address/host name and port number for the Netezza server.
4. Enter the name of the Netezza schema where you plan to create database objects.
5. Configure the path and file name for the ODBC log file.

6. Verify that you can connect to the Netezza database.

You can use the Microsoft ODBC Data Source Administrator to test the connection to the database. To test the connection, select the Netezza data source and click Configure. On the Testing tab, click Test Connection and enter the connection information for the Netezza schema.

## Connecting to an Oracle Database from Windows

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

### Configuring Native Connectivity

You can configure native connectivity to an Oracle database to increase performance.

The following steps provide a guideline for configuring native connectivity using Oracle Net Services or Net8. For specific connectivity instructions, see the database documentation.

1. Verify that the Oracle home directory is set.

For example:

```
ORACLE_HOME=C:\Oracle
```

2. Verify that the PATH environment variable includes the Oracle bin directory.

For example, if you install Net8, the path might include the following entry:

```
PATH=C:\ORANT\BIN;
```

3. Configure the Oracle client to connect to the database that you want to access.

Launch SQL\*Net Easy Configuration Utility or edit an existing `tnsnames.ora` file to the home directory and modify it.

**Note:** By default, the `tnsnames.ora` file is stored in the following directory: `<OracleInstallationDir>\network\admin`.

Enter the correct syntax for the Oracle connect string, typically `databasesname.world`. Make sure the SID entered here matches the database server instance ID defined on the Oracle server.

Here is a sample `tnsnames.ora` file. Enter the information for the database.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
          (PROTOCOL = TCP)
          (Host = mymachine)
          (Port = 1521)
        )
      )
    )
  (CONNECT_DATA =
    (SID = MYORA7)
    (GLOBAL_NAMES = mydatabase.world)
```



Here is a sample `tnsnames.ora` file to connect to Oracle using Oracle Connection Manager:

```
ORCL19C_CMAN =
(description=
(address_list=
(source_route=yes)
(address=(protocol=tcp) (host=inrh74ocm.mycompany.com) (port=1521))
(address=(protocol=tcp) (host=inrh74oradb.mycompany.com) (port=1521))
)
(connect_data=
(service_name=ORCL19C.mycompany.com)
)
)
```

4. Set the `NLS_LANG` environment variable to the locale, including language, territory, and character set, you want the database client and server to use with the login.

The value of this variable depends on the configuration. For example, if the value is `american_america.UTF8`, you must set the variable as follows:

```
NLS_LANG=american_america.UTF8;
```

To determine the value of this variable, contact the database administrator.

5. To set the default session time zone when the Data Integration Service reads or writes the Timestamp with Local Time Zone data, specify the `ORA_SDTZ` environment variable.

You can set the `ORA_SDTZ` environment variable to any of the following values:

- Operating system local time zone ('OS\_TZ')
- Database time zone ('DB\_TZ')
- Absolute offset from UTC (for example, '-05:00')
- Time zone region name (for example, 'America/Los\_Angeles')

You can set the environment variable at the machine where Informatica server runs.

6. If the `tnsnames.ora` file is not in the same location as the Oracle client installation location, set the `TNS_ADMIN` environment variable to the directory where the `tnsnames.ora` file resides.

For example, if the `tnsnames.ora` file is in the `C:\oracle\files` directory, set the variable as follows:

```
TNS_ADMIN= C:\oracle\files
```

7. Verify that you can connect to the Oracle database.

To connect to the database, launch SQL\*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

Use the connect string as defined in the `tnsnames.ora` file.

## Connecting to a PostgreSQL Database

For native connectivity, install the version of PostgreSQL client appropriate for the PostgreSQL database server version.

To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the PostgreSQL client and PostgreSQL database server. You must also install the same version of the PostgreSQL client on all machines that require it. To verify compatibility, contact PostgreSQL.

## Configuring Native Connectivity

You can configure native connectivity to a PostgreSQL database to increase performance.

The following steps provide a guideline for configuring native connectivity through PostgreSQL. For specific instructions, see the database documentation.

1. To configure connectivity for the PowerCenter Integration Service and PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. To install PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the `pg_service.conf` file in the following format:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter Repository Service database service name
```

To securely connect to PostgreSQL for the PowerCenter repository, set the `sslmode` to `require` along with the remaining required database properties in the `pg_service.conf` file in the following format:

```
sslmode=require
```

3. Set the `PGSERVICEFILE`, `PGHOME`, and `PATH` environment variables.

**PGSERVICEFILE.** Set the variable to the `pg_service.conf` file that contains the connection parameters for PostgreSQL database connection. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<InstallationDirectory>/pg_service.conf
```

Using a C shell:

```
$ setenv PGSERVICEFILE <InstallationDirectory>/pg_service.conf
```

**PGHOME.** Set the variable to the PostgreSQL installation path where you have installed the PostgreSQL client. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

Using a C shell:

```
$ setenv PGHOME /usr/pgsql-10
```

**PATH.** To run the PostgreSQL command line programs, set the variable to include the PostgreSQL client directory, `psql`. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

Using a C shell:

```
$ setenv PATH ${PGHOME}:${PATH}
```

4. Verify that you can connect to the PostgreSQL database.

To connect to the PostgreSQL database, launch the `psql` utility and enter the connectivity information.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a PostgreSQL database on Windows.

The following steps provide a guideline for configuring ODBC connectivity:

1. Create an ODBC data source using the DataDirect ODBC 7.1 wire protocol driver for PostgreSQL provided by Informatica.
2. Verify that you can connect to the PostgreSQL database using the ODBC data source.

For specific instructions, see the database documentation.

# Connecting to a Sybase ASE Database from Windows

For native connectivity, install the version of Open Client appropriate for your database version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

## Configuring Native Connectivity

You can configure native connectivity to a Sybase ASE database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. Verify that the SYBASE environment variable refers to the Sybase ASE directory.

For example:

```
SYBASE=C:\SYBASE
```

2. Verify that the PATH environment variable includes the Sybase OCS directory.

For example:

```
PATH=C:\SYBASE\OCS-15_0\BIN;C:\SYBASE\OCS-15_0\DLL
```

3. Configure Sybase Open Client to connect to the database that you want to access.

Use SQLEDT to configure the Sybase client, or copy an existing SQL.INI file (located in the %SYBASE%\INI directory) and make any necessary changes.

Select NLWNSCK as the Net-Library driver and include the Sybase ASE server name.

Enter the host name and port number for the Sybase ASE server. If you do not know the host name and port number, check with the system administrator.

4. Optionally, to connect to the SSL-enabled Sybase ASE database, perform the following tasks:

- Specify the following security attributes on the **Security** tab when you configure the data source name in the Sybase driver property:

Attribute	Description
Encryption Method	Indicates whether data is encrypted when transmitted over the network. Select SSL.
Validate Server Certificate	Indicates whether Informatica validates the certificate that is sent by the database server when SSL encryption is enabled.
Trust Store	The location and name of the trust store file.

Attribute	Description
Trust Store Password	The password to access the contents of the trust store file.
Host Name In Certificate	The host name that is established by the SSL administrator to validate the host name contained in the certificate.

- Add the Sybase ASE server certificate to the trusted.txt file in the Sybase ASE client.
- Add the following Sybase ASE server connection details to the SQL.INI file:

```
<server_instance_name>
    master tcp ether <host name> <port number> ssl="CN='common_name'"
    query tcp ether <host name> <port number> ssl="CN='common_name'"
```

5. Verify that you can connect to the Sybase ASE database.

To connect to the database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

User names and database names are case sensitive.

## Connecting to a Teradata Database from Windows

Install and configure native client software on the machines where the Data Integration Service and PowerCenter Integration Service process runs and where you install Informatica Developer and the PowerCenter Client. To ensure compatibility between Informatica and databases, use the appropriate database client libraries. You must configure connectivity to the following Informatica components on Windows:

- **Integration Service.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the Data Integration Service and PowerCenter Integration Service run. You must also configure ODBC connectivity.
- **Informatica Developer.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each machine that hosts a Developer tool that accesses Teradata. You must also configure ODBC connectivity.
- **PowerCenter Client.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each PowerCenter Client machine that accesses Teradata. Use the Workflow Manager to create a database connection object for the Teradata database.

**Note:** Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata.

## Configuring ODBC Connectivity

You can configure ODBC connectivity to a Teradata database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source for each Teradata database that you want to access.

To create the ODBC data source, use the driver provided by Teradata.

Create a System DSN if you start the Informatica service with a *Local System account* logon. Create a User DSN if you select the *This account* log in option to start the Informatica service.

2. Enter the name for the new ODBC data source and the name of the Teradata server or its IP address.

To configure a connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC data source, leave the DefaultDatabase field and the user name and password fields empty.

3. Configure Date Options in the Options dialog box.

In the Teradata Options dialog box, specify AAA for DateTime Format.

4. Configure Session Mode in the Options dialog box.

When you create a target data source, choose ANSI session mode. If you choose ANSI session mode, Teradata does not roll back the transaction when it encounters a row error. If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the Integration Service cannot detect the rollback and does not report this in the session log.

5. Verify that you can connect to the Teradata database.

To test the connection, use a Teradata client program, such as WinDDI, BTEQ, Teradata Administrator, or Teradata SQL Assistant.

## APPENDIX E

# Updating the DynamicSections Parameter of a DB2 Database

This appendix includes the following topics:

- [DynamicSections Parameter Overview, 342](#)
- [Setting the DynamicSections Parameter, 342](#)

## DynamicSections Parameter Overview

IBM DB2 packages contain the SQL statements to be executed on the database server. The DynamicSections parameter of a DB2 database determines the maximum number of executable statements that the database driver can have in a package. You can raise the value of the DynamicSections parameter to allow a larger number of executable statements in a DB2 package. To modify the DynamicSections parameter, connect to the database using a system administrator user account with BINDADD authority.

## Setting the DynamicSections Parameter

Use the DataDirect Connect for JDBC utility to raise the value of the DynamicSections parameter in the DB2 database.

To use the DataDirect Connect for JDBC utility to update the DynamicSections parameter, complete the following tasks:

- Download and install the DataDirect Connect for JDBC utility.
- Run the Test for JDBC tool.

## Downloading and Installing the DDconnect JDBC Utility

Download the DataDirect Connect for JDBC utility from the DataDirect download web site to a machine that has access to the DB2 database server. Extract the contents of the utility file and run the installer.

1. Go to the DataDirect download site:  
<http://www.datadirect.com/support/product-documentation/downloads>
2. Choose the Connect for JDBC driver for an IBM DB2 data source.

3. Register to download the DataDirect Connect for JDBC Utility.
4. Download the utility to a machine that has access to the DB2 database server.
5. Extract the contents of the utility file to a temporary directory.
6. In the directory where you extracted the file, run the installer.

The installation program creates a folder named testforjdbc in the installation directory.

## Running the Test for JDBC Tool

After you install the DataDirect Connect for JDBC Utility, run the Test for JDBC tool to connect to the DB2 database. You must use a system administrator user account with the BINDADD authority to connect to the database.

1. In the DB2 database, set up a system administrator user account with the BINDADD authority.
2. In the directory where you installed the DataDirect Connect for JDBC Utility, run the Test for JDBC tool (testforjdbc).
3. On the Test for JDBC Tool window, click Press Here to Continue.
4. Click Connection > Connect to DB.
5. In the Database field, enter the following text:

```
jdbc:datadirect:db2://  
HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
```

*HostName* is the name of the machine hosting the DB2 database server.

*PortNumber* is the port number of the database.

*DatabaseName* is the name of the DB2 database.

6. In the User Name and Password fields, enter the system administrator user name and password you use to connect to the DB2 database.
7. Click Connect, and then close the window.

# INDEX

## A

- AddLicense (infacmd)
  - troubleshooting [238](#)
- Analyst Service
  - after creating [278](#)
  - configuring [276](#)
  - creating [276](#)
  - prerequisites [247](#)
  - temporary directories [247](#)
- application services
  - Content Management Service [54](#)
  - Analyst Service [53](#)
  - Data Integration Service [56](#), [71](#)
  - installation requirements [30](#), [40](#)
  - Metadata Manager Service [62](#)
  - Model Repository Service [67](#), [72](#)
  - monitoring Model Repository Service [71](#)
  - ports [27](#), [39](#)
  - products [48](#)
  - Search Service [75](#)

## B

- back up files
  - before installing [31](#), [42](#)
  - before upgrading [31](#), [42](#)
- before installing the clients
  - overview [283](#)
  - verifying installation requirements [283](#)
  - verifying minimum system requirements [283](#)

## C

- catalina.out
  - troubleshooting installation [236](#)
- clients
  - configuring for secure domains [285](#)
- code page compatibility
  - application services [242](#)
  - locale [242](#)
- configuration
  - domains [242](#)
  - environment variables [243](#)
  - environment variables on UNIX [244](#)
  - Kerberos files [82](#)
- connecting
  - Integration Service to IBM DB2 (Windows) [305](#), [332](#)
  - Integration Service to Informix (UNIX) [307](#)
  - Integration Service to Informix (Windows) [332](#)
  - Integration Service to JDBC data sources (UNIX) [322](#)
  - Integration Service to Microsoft Access [333](#)
  - Integration Service to Microsoft SQL Server [333](#)
  - Integration Service to ODBC data sources (UNIX) [322](#)

- connecting (*continued*)
  - Integration Service to Oracle (UNIX) [311](#)
  - Integration Service to Oracle (Windows) [336](#)
  - Integration Service to PostgreSQL (UNIX) [313](#)
  - Integration Service to PostgreSQL (Windows) [337](#)
  - Integration Service to Sybase ASE (UNIX) [317](#)
  - Integration Service to Sybase ASE (Windows) [339](#)
  - Microsoft Excel to Integration Service [333](#)
  - UNIX databases [304](#)
  - Windows databases [331](#)
  - Windows using JDBC [331](#)
- connections
  - creating database connections [249](#), [254](#)
  - IBM DB2 properties [250](#)
  - Microsoft Azure SQL Database properties [250](#)
  - Microsoft SQL Server properties [251](#)
  - Oracle properties [252](#)
  - PostgreSQL properties [253](#)
- Content Management Service
  - configuring [274](#)
  - creating [274](#)

## D

- Data Integration Service
  - after creating [264](#)
  - configuring [261](#)
  - creating [261](#)
  - host file configuration [264](#)
- data object cache
  - database requirements [57](#)
  - IBM DB2 database requirements [57](#)
  - Microsoft Azure SQL database requirements [57](#)
  - Microsoft SQL Server database requirements [57](#)
  - Oracle database requirements [58](#)
- database clients
  - configuring [78](#)
  - environment variables [78](#)
  - IBM DB2 client application enabler [77](#)
  - Microsoft SQL Server native clients [77](#)
  - Oracle clients [77](#)
  - PostgreSQL client [77](#)
  - Sybase open clients [77](#)
- database connections
  - creating [249](#)
- database preparations
  - repositories [48](#)
- database requirements
  - data object cache [57](#)
  - Model repository [68](#)
  - PowerCenter repository [72](#)
  - profiling warehouse [58](#)
  - reference data warehouse [54](#)
  - workflow database [59](#)



- database user accounts
  - guidelines for setup [48](#)
- databases
  - connecting to (UNIX) [304](#)
  - connecting to (Windows) [331](#)
  - connecting to IBM DB2 [305](#), [332](#)
  - connecting to Informix [307](#), [332](#)
  - connecting to Microsoft Access [333](#)
  - connecting to Microsoft SQL Server [333](#)
  - connecting to Netezza (UNIX) [309](#)
  - connecting to Netezza (Windows) [335](#)
  - connecting to Oracle [311](#), [336](#)
  - connecting to PostgreSQL [313](#), [337](#)
  - connecting to Sybase ASE [317](#), [339](#)
  - connecting to Teradata (UNIX) [319](#)
  - connecting to Teradata (Windows) [340](#)
  - repository [48](#)
  - testing connections [78](#)
- dbs2 connect
  - testing database connections [78](#)
- debug logs
  - troubleshooting the installation [236](#)
- Developer tool
  - third-party software requirements [283](#)
- DISPLAY
  - environment variables [42](#)
- domain configuration repository
  - IBM DB2 database requirements [50](#), [68](#)
  - Microsoft Azure SQL database requirements [51](#), [69](#)
  - Microsoft SQL Server database requirements [51](#), [69](#)
  - Oracle database requirements [51](#)
  - preparing databases [49](#)
  - Sybase ASE database requirements [52](#)
  - troubleshooting [237](#)
- Domain configuration repository
  - PostgreSQL database requirements [52](#)
- domains
  - configuring [242](#)
  - overview [19](#)
  - ports [27](#), [39](#)

## E

- environment variables
  - configuring [243](#)
  - configuring clients [285](#)
  - configuring on UNIX [244](#)
  - database clients [78](#)
  - INFA\_TRUSTSTORE [285](#)
  - INFA\_TRUSTSTORE\_PASSWORD [285](#)
  - installation [32](#), [42](#)
  - LANG [242](#)
  - LANG\_C [242](#)
  - LC\_ALL [242](#)
  - LC\_CTYPE [242](#)
  - library paths on UNIX [244](#)
  - locale [242](#)
  - UNIX [243](#)
  - UNIX database clients [78](#)

## G

- graphical mode
  - installing Informatica clients [284](#)
  - installing Informatica services [157](#)

## H

- host file
  - Data Integration Service [264](#)
- HTTPS
  - installation requirements [33](#), [43](#)

## I

- i10Pi
  - UNIX [101](#)
  - Windows [105](#)
- IATEMPDIR
  - environment variables [32](#), [42](#)
- IBM DB2
  - connecting to Integration Service (Windows) [305](#), [332](#)
  - setting DB2CODEPAGE [332](#)
  - setting DB2INSTANCE [332](#)
  - single-node tablespaces [73](#)
- IBM DB2 database requirements
  - data object cache [57](#)
  - domain repository [50](#), [68](#)
  - Metadata Manager repository [63](#)
  - Model repository database [50](#), [68](#)
  - PowerCenter repository [73](#)
  - profiling warehouse [58](#)
  - reference data warehouse [55](#)
  - workflow repository [60](#)
- infacmd
  - adding nodes to domains [237](#)
  - pinging objects [238](#)
- infasetup
  - defining domains [237](#)
  - defining worker nodes [237](#)
- Informatica Administrator
  - logging in [248](#)
- Informatica clients
  - installing in graphical mode [284](#)
  - installing in silent mode [289](#)
  - uninstalling [292](#), [294](#)
- Informatica Developer
  - configuring local workspace directory [286](#)
  - installing languages [285](#)
  - local machines [286](#)
  - remote machines [286](#)
- Informatica server
  - uninstalling [292](#)
- Informatica services
  - installing in graphical mode [157](#)
  - installing in silent mode [231](#)
  - starting and stopping on UNIX [297](#)
  - troubleshooting [238](#)
- Informix
  - connecting to Integration Service (UNIX) [307](#)
  - connecting to Integration Service (Windows) [332](#)
- installation
  - backing up files before [31](#), [42](#)
- installation logs
  - descriptions [236](#)
- installation requirements
  - application service requirements [30](#), [40](#)
  - environment variables [32](#), [42](#)
  - keystore files [33](#), [43](#)
  - port requirements [27](#), [39](#)
  - truststore files [33](#), [43](#)
- isql
  - testing database connections [78](#)

## J

JDBC  
connecting to (Windows) [331](#)  
JDBC data sources  
connecting to (UNIX) [322](#)  
JRE\_HOME  
environment variables [32, 42](#)

## K

Kerberos authentication  
configuration files [82](#)  
creating keytab files [88](#)  
creating service principal names [88](#)  
generating keytab file name formats [83](#)  
generating SPN formats [83](#)  
troubleshooting [248](#)  
Kerberos SPN Format Generator [85](#)  
keystore files  
installation requirements [33, 43](#)  
keytab files  
Kerberos authentication [83, 88](#)

## L

LANG  
environment variables [242](#)  
locale environment variables [32, 42](#)  
languages  
client tools [285](#)  
LC\_ALL  
environment variables [242](#)  
locale environment variables [32, 42](#)  
LC\_CTYPE  
environment variables [242](#)  
library paths  
environment variables [32](#)  
library requirements  
Windows [38](#)  
license keys  
verifying [36, 46](#)  
licenses  
adding [238](#)  
Linux  
database client environment variables [78](#)  
locale environment variables  
configuring [242](#)  
localhost  
Data Integration Service [264](#)  
log files  
catalina.out [236](#)  
debug logs [236](#)  
installation [235](#)  
installation logs [236](#)  
node.log [236](#)  
types [235](#)  
login  
troubleshooting [248](#)

## M

Metadata Manager repository  
heap sizes [63](#)  
IBM DB2 database requirements [63](#)

Metadata Manager repository (*continued*)  
Microsoft SQL Server database requirements [64](#)  
optimizing IBM DB2 databases [63](#)  
Oracle database requirements [65](#)  
system temporary tablespaces [63](#)  
Metadata Manager Service  
after creating [274](#)  
configuring [270](#)  
creating [270](#)  
creating repository contents [274](#)  
split domain [66](#)  
split domain considerations [66](#)  
Microsoft Access  
connecting to Integration Service [333](#)  
Microsoft Azure SQL database requirements  
data object cache [57](#)  
domain configuration repository [51, 69](#)  
reference data warehouse [55](#)  
workflow database [60](#)  
Microsoft Excel  
connecting to Integration Service [333](#)  
using PmNullPasswd [333](#)  
using PmNullUser [333](#)  
Microsoft SQL Server  
connecting from UNIX [308](#)  
connecting to Integration Service [333](#)  
Microsoft SQL Server database requirements  
data object cache [57](#)  
domain configuration repository [51, 69](#)  
Metadata Manager repository [64](#)  
PowerCenter repository [73](#)  
profiling warehouse [59](#)  
reference data warehouse [55](#)  
workflow repository [60](#)  
minimum system requirements  
nodes [30, 40](#)  
Model repository  
database requirements [68](#)  
IBM DB2 database requirements [50, 68](#)  
Oracle database requirements [70](#)  
PostgreSQL database requirements [70](#)  
users [260](#)  
Model Repository Service  
after creating [259](#)  
configuring [256](#)  
creating [256](#)

## N

Netezza  
connecting from Informatica clients(Windows) [335](#)  
connecting from Integration Service (Windows) [335](#)  
connecting to Informatica clients (UNIX) [309](#)  
connecting to Integration Service (UNIX) [309](#)  
node.log  
troubleshooting installation [236](#)  
nodes  
troubleshooting [237](#)  
normal mode  
PowerCenter Repository Service [266](#)

## O

ODBC data sources  
connecting to (UNIX) [322](#)  
connecting to (Windows) [331](#)

- odbc.ini file
  - sample [324](#)
- operating mode
  - PowerCenter Repository Service [266](#)
- optimization
  - PowerCenter repository [73](#)
- Oracle
  - connecting to Integration Service (UNIX) [311](#)
  - connecting to Integration Service (Windows) [336](#)
- Oracle database requirements
  - data object cache [58](#)
  - domain configuration repository [51](#)
  - Metadata Manager repository [65](#)
  - Model repository [70](#)
  - PowerCenter repository [73](#)
  - profiling warehouse [59](#)
  - reference data warehouse [55](#)
  - workflow repository [61](#)
- Oracle Net Services
  - using to connect Integration Service to Oracle (UNIX) [311](#)
  - using to connect Integration Service to Oracle (Windows) [336](#)
- overview
  - before installing the clients [283](#)

## P

- patch requirements
  - installation [26](#)
  - Windows [38](#)
- PATH
  - environment variables [32](#)
- pg\_service.conf
  - PostgreSQL database requirements [74](#)
- PGSERVICEFILE environment variable
  - PostgreSQL database requirements [74](#)
- Ping (infacmd)
  - troubleshooting [238](#)
- port requirements
  - installation requirements [27, 39](#)
- ports
  - application services [27, 39](#)
  - domains [27, 39](#)
  - requirements [27, 39](#)
- PostgreSQL
  - connecting to Integration Service (UNIX) [313](#)
  - connecting to Integration Service (Windows) [337](#)
- PostgreSQL database requirements
  - Domain configuration repository [52](#)
  - Model repository [70](#)
  - pg\_service.conf [74](#)
  - PGSERVICEFILE environment variable [74](#)
  - PowerCenter repository [74](#)
  - workflow database [61](#)
- PowerCenter Client
  - third-party software requirements [284](#)
- PowerCenter Integration Service
  - after creating [270](#)
  - configuring [268](#)
  - creating [268](#)
- PowerCenter repository
  - database requirements [72](#)
  - IBM DB2 database requirements [73](#)
  - Microsoft SQL Server database requirements [73](#)
  - optimizing IBM DB2 databases [73](#)
  - Oracle database requirements [73](#)
  - Oracle RAC [73](#)
  - PostgreSQL database requirements [74](#)

- PowerCenter repository (*continued*)
  - Sybase ASE database requirements [75](#)
  - users [267](#)
- PowerCenter Repository Service
  - after creating [266](#)
  - configuring [264](#)
  - creating [264, 265](#)
  - normal mode [266](#)
- pre-installation
  - i10Pi on UNIX [101](#)
  - i10Pi on Windows [105](#)
  - services on Windows [37](#)
- profiling warehouse
  - database requirements [58](#)
  - IBM DB2 database requirements [58](#)
  - Microsoft SQL Server database requirements [59](#)
  - Oracle database requirements [59](#)

## R

- reference data warehouse
  - database requirements [54](#)
  - IBM DB2 database requirements [55](#)
  - Microsoft Azure SQL database requirements [55](#)
  - Microsoft SQL Server database requirements [55](#)
  - Oracle database requirements [55](#)
- repositories
  - configuring native connectivity [76](#)
  - installing database clients [77](#)
  - preparing databases [48](#)
- repository content creation
  - Metadata Manager Service [274](#)

## S

- samples
  - odbc.ini file [324](#)
- Search Service
  - configuring [278](#)
  - creating [278](#)
- secure domains
  - configuring clients [285](#)
- Service Manager
  - log files [236](#)
- service principal names
  - creating [88](#)
  - Kerberos authentication [83](#)
- services
  - pre-installation tasks on Windows [37](#)
- silent mode
  - installing Informatica clients [289](#)
  - installing Informatica services [231](#)
- source databases
  - connecting through JDBC (UNIX) [322](#)
  - connecting through ODBC (UNIX) [322](#)
- split domain for Metadata Manager
  - considerations [66](#)
  - definition [66](#)
- SPN [83](#)
- sqlplus
  - testing database connections [78](#)
- Sybase ASE
  - connecting to Integration Service (UNIX) [317](#)
  - connecting to Integration Service (Windows) [339](#)
- Sybase ASE database requirements
  - domain configuration repository [52](#)

Sybase ASE database requirements (*continued*)

PowerCenter repository [75](#)

system requirements

application services [30](#), [40](#)

minimum [25](#), [38](#)

## T

tablespaces

single nodes [73](#)

target databases

connecting through JDBC (UNIX) [322](#)

connecting through ODBC (UNIX) [322](#)

Teradata

connecting to Informatica clients (UNIX) [319](#)

connecting to Informatica clients (Windows) [340](#)

connecting to Integration Service (UNIX) [319](#)

connecting to Integration Service (Windows) [340](#)

third-party software requirements

Developer tool [283](#)

PowerCenter Client [284](#)

troubleshooting

creating domains [237](#)

domain configuration repository [237](#)

Informatica services [238](#)

joining domains [237](#)

Kerberos authentication [248](#)

licenses [238](#)

logging in [248](#)

pinging domains [238](#)

truststore files

installation requirements [33](#), [43](#)

## U

uninstallation

rules and guidelines [292](#)

UNIX

connecting to JDBC data sources [322](#)

connecting to ODBC data sources [322](#)

UNIX (*continued*)

database client environment variables [78](#)

database client variables [78](#)

environment variables [243](#)

i10Pi [101](#)

Kerberos SPN Format Generator [85](#)

library paths [244](#)

pre-installation [101](#)

starting and stopping Informatica services [297](#)

user accounts [33](#)

upgrades

backing up files before [31](#), [42](#)

user accounts

Model repository [260](#)

PowerCenter repository [267](#)

UNIX [33](#)

Windows [43](#)

user principal names

formatting [88](#)

## W

Windows

i10Pi [105](#)

installing Informatica clients in graphical mode [284](#)

installing Informatica services in graphical mode [157](#)

library requirements [38](#)

patch requirements [38](#)

pre-installation [105](#)

user accounts [43](#)

workflow

IBM DB2 database requirements [60](#)

Microsoft SQL Server database requirements [60](#)

Oracle database requirements [61](#)

workflow database

Microsoft Azure SQL database requirements [60](#)

PostgreSQL database requirements [61](#)

workflows

database requirements [59](#)